

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-174797

(43)Date of publication of application : 23.06.2000

(51)Int.Cl.

H04L 12/46
H04L 12/28
G11B 20/10
H04L 9/32
H04L 12/66
H04L 29/06

(21)Application number : 11-209836

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 23.07.1999

(72)Inventor : SAITO TAKESHI
TAKAHATA YOSHIKI

(30)Priority

Priority number : 10292824

Priority date : 30.09.1998

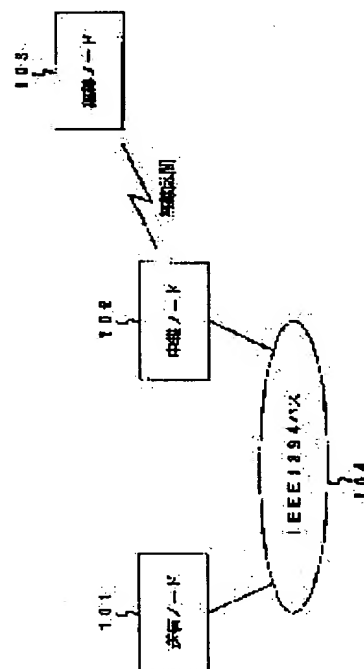
Priority country : JP

(54) REPEATER AND COMMUNICATION EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a repeater capable of a contents protection procedure between equipment not connected to the same network.

SOLUTION: This repeater is connected to a first network 104 and a second network and is provided with a function for presenting the equipment 103 on the second network to the side of the first network 104 as the one on the present repeater 102, the function for transmitting a corresponding control command to the equipment 103 in the case of receiving the control command addressed to the equipment 103 from the equipment 101 on the first network 104, the function for transmitting contents protection information to the equipment 103 without changing it in the case of receiving it addressed to the equipment 103 from the equipment 101 and the function for transmitting contents to the equipment 103 without changing them in the case of receiving the contents protected by a contents key obtained from the previous contents protection information from the equipment 101 to the equipment 103.



BEST AVAILABLE COPY

LEGAL STATUS

[Date of request for examination]

03.12.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

(A) 報時開公 (12) 許時開公 (19) 日本國特許庁 (JP)

(11) 特許出版公開番号

特開2000-174797

(P2000-174797A)

(43)公開日 平成12年6月23日(2000.6.23)

(31) InCl ⁺	識別記号	F ₁	F-T ₁ (参考)
H04L 12/46		H04L 11/00	310C
	12/28	G1B 20/10	H
G1B 20/10		H04L 9/00	673A
H04L 9/32			675D
12/68		11/20	B

審査請求 未請求 請求項の項17 OL (全 60 頁) 最終頁に記

審査請求 未請求 請求項の数17 O.L (全 60 頁) 最終頁に脱ぐ

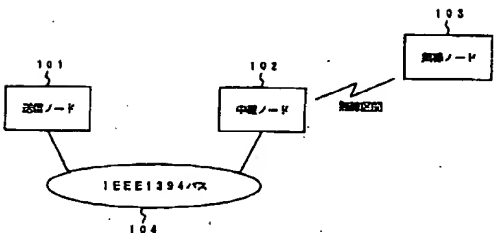
(21) 出版番号	特選平11-209838
(22) 出版日	平成11年7月23日 (1998. 7. 23)
(31) 報告種主番号	特選平10-232824
(32) 優先日	平成10年9月30日 (1998. 9. 30)
(33) 優先種主国	日本 (J P)
(71) 出願人	000006078 株式会社東芝 神奈川県川崎市幸区堀川町2番地 有藤 健
(72) 発明者	神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝研究開発センター内 高田 由彰
(73) 発明者	神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝研究開発センター内 100036479 伊藤士 敏彦 (外6名)
(74) 代理人	

(54) 【発明の名称】 中継装置及び通信装置

(57) 【要約】

【保題】 同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置を提供すること。

【解説手配】第1のネットワーク104と第2のネットワーク1は接続され、第2のネットワーク上の装置103を自己装置102とするものとして、第1のネットワーク104上の装置101から装置103宛の制御コマンドを受信した場合、これに対応する制御コマンドを装置103へ送信する機能と、装置101から装置103宛のコントロール信号を受信した場合、これに変更を加えずに装置103へ送信する機能とを有する。



【特許請求の範囲】

【請求項1】第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

ユニットを、自中継装置上のもとして前記第1のネットワーク側に開示する代型構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第1のネットワーク側から受信する制御コマンド受信手段と、

この前記コマンンド受信手段で受信した前記前記コマンンド信号に対応した信号を前記第2のネットワーク上の装置又はサービス又はサブユニット宛に送信する前記コマンンド送信手段と、

前記第1のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサーバ又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテナ保護情報受信手段で受信したコンテナ保護情報に、変更を加えず、前記第2のネットワーク上の送信機又はサーバ又はサブユニット宛に転送するコンテナ保護情報伝送手段とを具備したことを特徴とするコンピュータ装置。

【請求項2】第1のネットワークに接続された第1のインタフェース手段と、
第2のネットワークに接続された第2のインタフェース手段と、

第1及び第2のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものであるとして各々他方のネットワーク側に開示する代理構成手段と、

この表題又はサービスマスはサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド
信号に対応した信号を、前記変換手段で開示したネッ
トワークと異なるネットワーク上の装置又はサーバス
タはサブユニット宛に送信する制御コマンド送信手段

前記第1又は第2のネットワーク上の装置から、前記代理情報手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受は手段で受信したコンテンツ保護情報に変更を加えず、前記地方のネットワーク上の装置又はサーバ又はサブユニット宛に転送するコンテンツ保護情報転送手段と、

前記第1又は第2のネットワーク上の装置から、前記変換手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られる

コンテンツ上で保護されたコンテンツを受信するコンテンツ受信手段と、

このコンテンツ受領手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサーバ又はサブユニット宛に伝送するコンテンツ伝送手段とを具備したことを特徴とする中継装置。

【請求項3】前記コンテナツプ保護情報は、前記第1のネットワーク上の装置又はサーバ又はサブユニットと、前記第2のネットワーク上の装置又はサーバ又はサブユニット間の認証及び鍵交換を含むコンテナツプ保護の手続きに関する情報であることを特徴とする請求項2に記載の非特許文献。

【結果事項4】第1のネットワークに接続された第1のインタフェース手段、
第2のネットワークに接続された第2のインタフェース手段と、

第1及び第2のネットワーク上の装置又はサーバ又はサブリユニットを、自律継続性上のものでして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサーバ又はサブリユニットの制御ユニットに格納された代理構成手段で開示したネットワーク内から受信する制御コマンドを受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド情報に対しては、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサーバ又はサブユニット宛に送信する制御コマンド送信手段上。

前記第1のネットワーク上の装置又はサービス又はサブ
ユニットと、自ynch装置の間で、コンテンツ保護の手続
きを行う第1のコンテンツ保護手段と、

前記第2のネットワーク上の装置又はサーバ又はサブリユニットと、自中継装置の間で、コンテンツ保護の手段と、きを行う第2のコンテンツ保護手段と、

前記第1又は第2のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自律構築服上の装置又はサーバ又はサブユニット宛であり、前記第1又は第2のいずれか一方のコンテンツ保護手段に基いて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第1又は第2のいずれか他方のコンテンツ保護手段に送る。ここで、暗号化し、前記第1又は第2のいずれか他方のネットワーク上の装置又はサーバ又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項5】前記第1のコンデンツ保護手段と、前記第2のコンデンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる制御部に基づくものであることを特徴とする請求項4に記載の中継装置。

ッ送信手段は同一のLSIに封止されていることを特徴とする請求項4に記載の中継装置。

【請求項7】 前記第1のコンテンツ保護手段における前記コンテンツ保護の手段として使用する第1の鍵情報と、前記第2のコンテンツ保護手段における前記コンテンツ保護の手段として使用する第2の鍵情報とを同一のものとすることを特徴とする請求項4に記載の中継装置。

【請求項8】 前記第1又は第2のいずれか一方のコンテンツ保護手段における前記コンテンツ保護の手段は、所定の鍵情報を用いて、コンテンツ単位又はサブユニット単位で行なうことを特徴とする請求項4に記載の中継装置。

【請求項9】 前記第1及び第2のネットワーク上の装置又はサブユニットから、該装置の認証フローネットワークの有無を含む構成情報を受信する構成情報受信手段と、

前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサブユニットはサブユニットの構成認識を行う構成認識手段とを更に具備したことを特徴とする請求項4または5に記載の中継装置。

【請求項10】 第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

前記第1のネットワーク上の装置又はサブユニット又はサブユニットと、自中継装置の間で、コンテンツ保護の手段きを行う第1のコンテンツ保護手段と、

前記第2のネットワーク上の装置又はサブユニット又はサブユニットと、自中継装置の間で、コンテンツ保護の手段きを行う第2のコンテンツ保護手段と、

前記第1又は第2のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサブユニット又はサブユニットと宛てて、前記第1又は第2のいずれか一方のコンテンツ保護手段に宛てて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第1又は第2のいずれか一方のコンテンツ保護手段に宛てて暗号化し、前記第1又は第2のいずれか一方のネットワーク上の装置又はサブユニット又はサブユニット宛に送信するコンテンツ送信手段とを具備し、

前記第1のコンテンツ保護手段における前記コンテンツ保護の手段として使用する第1の鍵情報と、前記第2のコンテンツ保護手段における前記コンテンツ保護の手段として使用する第2の鍵情報とを同一のものとすることを特徴とする中継装置。

【請求項11】 ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサブユニットまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段きを行なうコヒーレントな処理手段と、

なうコヒーレントな処理手段と、

前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの宛先チャネルを介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、

前記ネットワーク上の他の装置から、前記宛先チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサブユニットまたはサブユニットまたはサブユニットについての問合せを受信する受信手段と、

この問合せに応じて、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはサブユニットについての通知をする通知手段とを具備することを特徴とする通信装置。

【請求項12】 ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサブユニットまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段きを行なうコヒーレントな処理手段と、

前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの宛先チャネルを介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、

前記ネットワーク上の他の装置に対して、前記宛先チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサブユニットまたはサブユニットまたはサブユニットについての問合せを送信する送信手段と、

前記ネットワーク上の他の装置から、前記問合せに応じて該当するサービスまたはサブユニットまたはサブユニットについて通知を受信する受信手段とを具備することを特徴とする通信装置。

【請求項13】 ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、

前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段きを行なうコヒーレントな処理手段とを具備し、

前記所定のコンテンツ保護手段きを行なう場合には、これを前記フローの単位で行なうことを特徴とする通信装置。

【請求項14】 前記所定のコンテンツ保護手段きを含む

れる少なくとも一部の手段きにおいてやり取りされる情報に前記フローの識別子を付与することを特徴とする請求項21に記載の通信装置。

【請求項15】 ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサブユニットまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段きを行なうコヒーレントな処理手段と、

前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの宛先チャネルを介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、

前記所定のコンテンツ保護手段きに含まれる少なくとも一部の手段きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサブアドレス、サブユニット、宛先チャネルもしくはサブアドレスの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子を含む少なくとも一つを付与することを特徴とする通信装置。

【請求項16】 第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

第1のネットワーク上の装置またはサブユニットまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段きを行う第1のコヒーレントな処理手段と、

第2のネットワーク上の装置またはサブユニットまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段きを行う第2のコヒーレントな処理手段と、

前記第1のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第1のインタフェース手段から受信された前記暗号化されたデータを、前記第1のコヒーレントな処理手段で暗号化されたデータと、前記第1のコヒーレントな処理手段で提供されるコンテンツ保護用の鍵で暗号化されたデータと、

前記第2のインタフェース手段から暗号化されたデータと、前記第2のコヒーレントな処理手段で提供されるコンテンツ保護用の鍵で暗号化されたデータと、

前記第1のインタフェース手段から暗号化されたデータと、前記第2のインタフェース手段から暗号化されたデータとを具備したことを特徴とする中継装置。

【請求項17】 前記第2のネットワーク上の装置または

サブユニットまたはサブユニットを、自中継装置上のものと、前記第1のネットワーク側に提示するとともに、

前記第1のネットワーク側の装置から、自中継装置上のものと提示して開示した装置またはサブユニットまたはサブユニットの情報を前記第2のネットワーク上の装置またはサブユニットまたはサブユニット宛に送信する送信手段と、

前記第1のネットワーク上の装置またはサブユニットまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に提示するとともに、前記第2のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサブユニット宛に送信する送信手段と、

前記第1のネットワーク上の装置またはサブユニットまたはサブユニットと、この情報に基いた内容の情報を前記第1のネットワーク上の装置またはサブユニットまたはサブユニット宛に送信する代理構成手段を更に具備し、

前記代理構成手段は、前記第1または第2の一方のネットワーク上の装置と、前記第1または第2の一方のネットワーク上の装置またはサブユニットまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段きを行う場合には、前記第1または第2の一方のコヒーレントな処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手段きを行うとともに、前記第1または第2の他方のネットワーク上の装置またはサブユニットまたはサブユニットと該所定のコンテンツ保護手段きを行うことを特徴とする請求項24に記載の中継装置。

【発明の詳細な説明】

【0001】 本発明は、IEEE1394バスや無線ネットワーク等のネットワーク間のデータ転送を中継する中継装置及びIEEE1394バスや無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【0002】 従来の技術 近年、デジタル放送の開始や、デジタルAV機器の普及等、いわゆる「家庭AV環境のデジタル化」が大きな注目を集めている。デジタルAVデータは、様々な圧縮が可能、アルチメディアデータとしても処理可能な、何回再生しても劣化がない、等の優れた特徴をもち、今後その用途はますます広がっていくものと考えられる。

【0003】 しかしながら、このデジタルAV技術には、反面、「コンテンツの不正コピーが容易に行える」という側面もある。すなわち、どのようなデジタルコンテンツについても、原則的に「コピー」で、元どおりの品質の、しかも本来本物にわたって一切劣化のない複製が作れてしまうため、いわゆる「不正コピー」の問題が発生する。

【0004】 この「不正コピー」を防ぐための技術がい

へ伝送された暗号化データの鍵に関する情報（鍵やシー
ド料）を、他方のネットワークへそのまま伝送すること
により、他方のネットワーク上の装置では暗号化鍵の
再生が可能となるため、コンテナ受取手続とコンテナ
手続併行手段との間の暗号復号機能および暗号化機能が
必要でない。中継装置の大幅なコストの低減と、処理速
度の高速化を図ることが可能となる。

【0002.】また、好ましくは、他方のネットワーク上の装置と、叩字化されたデータの転送を行っている場合には、他方のネットワーク上の他の装置からの、叩字化が必要となるデータの送信要求は拒否するようにしてもよい。このようにすれば、他方のネットワーク側においても、異なる叩字化されたデータ転送を未然に防止することが可能となる。

【0002】乍ましくは、前記第1又は第2のいずれかの手続のコーディング手段におけるコーディング手段は、他のコーディング手段を用いて、コーディング単位又はサブサービス単位又はサブグループ単位で行なうようにしてもよい、これによって、他のコーディングコードの装置との間で、複数の呼号紐を定義できるようにするため、呼号化されたデータを同時に低減させることが可能となり、一方のネットワーク上の装置から複数の呼号化データが低減される場合あるいは一方のネットワーク上に複数の装置がある場合等への対応が可能となる。

(10023) 乍ましくは、前記2)及び前2のネットワーク上の装置又はサーバ又はサブユニットから、該装置の認証ソフトウェア(厳密証明)の有無を含む構成情報を受信する構成情報受信手段と、前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサーバ又はサブユニットの構成認識を行う構成認識手段とを有する手段が構成するようになり、これによって、代理構成手段が構成する代理サーバを、自動的に構成することのできるようになり、もって、コンテンツ保護手続きに至る手順のプログラムレベルでの実現が可能になる。

【0024】また、好ましくは、前記代理構成手段は、情報第1のネットワークの装置に対してデータを送信する際、あらかじめ情報第1のネットワークの装置に対して自中継装置が代理構成している該データを送信する装置またはサーバへこれまたはその通知を受けるようにしてもよい、このような、この通知を受信する第1のネットワーク上の装置に対して、どこに税金要求を出せばよいかを通知すること可能になる。

【0002】本発明（請求項1）に係る中継装置は、第1のネットワークには接続された第1のインタフェース手段と、第2のネットワークには接続された第2のインタフェース手段と、前記第1のネットワーク上の装置又はサーバと又はサーバユニットと、自律統装置の別で、コンテンツ保護の手続きを行う第1のコンテンツ保護手段と、前記第2のネットワーク上の装置又はサーバ又は

12

サブユニットと、自中継装置の間で、コンデンツ保護の手続きを行う第2のコンデンツ保護手段と、前記第1又は第2のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット境であり、前記第1又は第2のいずれか一方のコンデンツ保護手段に基づいて暗号化されたコンデンツを受信するコンデンツ受信手段と、前記コンデンツを受信手段で受信したコンデンツを、前記第1又は第2のいずれか一方のコンデンツ保護手段に基づいて暗号化し、前記第1又は第2のいずれか一方のネットワーク上の装置又はサービス又はサブユニット境に送信するコンデンツ送信手段とを具備し、前記第1のコンデンツ保護手段における前記コンデンツ保護の手続きで使用する第1の鍵情報と、前記第2のコンデンツ保護手段における前記コンデンツ保護の手続きで使用する第2の鍵情報とを同一のものとする。と特徴とする。

【0020】本発明（請求項1）に係る通信装置は、ネットワークに接続されたインターネットエース手段と、前記ネットワーク上の他の装置またはインターネットエースまたはサーバとの間で、少なくとも通信手続きおよびまたはデータ交換手続きを含む所定のコンテンツ保護手続きを行なうコンピュータロジック処理手段と、前記ネットワーク上の他の装置に対し、自通信装置のアドレスを付与した呼号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび送信コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、前記ネットワーク上の他の装置から、前記仮想チャネルを介してまたは前記識別子付きのデータを送信してコンテンツを転送しているサーバまたはサーバエースまたはサーバについての問合せを受ける受信手段と、この問合せに応答して前記ネットワーク上の他の装置に対し、該当するサーバまたはサーバエースまたはサーバについての通知を送る通知手段とを具備することと特徴とする。

【0002】本発明（請求項1、2）に係る通信装置は、ネットワーク上に接続されたネットワークスーエス手段と、前記ネットワーク上の他の装置またはネットワークスーエス手段と、前記ネットワーク上で、少なくとも一部は通信手段をおよびまたは通信手段を含む所定のコンテンツ保護手段を行なうコピードロパクシヨニ処理手段と、前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが与えられた暗号化されたコンテンツを、ネットワーク上の仮記憶チャネル上をとりまは該ネットワーク上の他の装置が該コンテンツを一箇に識別可能な識別子が付与された形で、受取るコンテンツ受信手段と、前記ネットワーク上の他の装置に対して、前記仮記憶チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを伝送するサービスエスまたはサブエスまたはプラグインについての情報を送るサブエス手段と、前記ネットワーク上の他の装置から、前記問合せに該当する

13
 ザービスまたはソフトウェアについての
 通知を受領する受領手段とを具備するこ
 とを特徴とする。

【0020】本発明によれば、特定の低次元セルで転送されている暗号化データの送信、あるいは受信がそれらのサブユニットあるいはブロックを特定することが可能となり、以後の認証・鍵交換で、このサブユニット（あるいはブロック）から送信、あるいは受信されているデータに関する認証・鍵交換を行ったと明示することが可能となり、もって同一ノード同士でも、同時に複数の転送を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【0002】本発明（請求項13）に係る通信装置は、ネットワークに接続されたインターネットエース手段と、前記ネットワーク上の他の装置に対して、呼号されたコンテナットを、送信ポート、受信ポート、受信ポートおよび受信ポートの組で識別されるフローを介して送達または受信するコンテナット転送手段と、前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも二投送手段とよびまたは般交換手段を含む所定のコンテナット保護書きを行なうコピーングコソクノ処理手段とを具備し、前記所定のコンテナット保護手段書きを行なう場合には、これを前記コピーングの手段で行なうことを特徴とする。

【00303】好ましくは、前記所定のコンテンツ保護手段
 統きに含まれる少なくとも一部の手続きにおいてやり取
 りされる情報に前記フローの識別子を付与するようにし
 てよい。

【0031】本發明によれば、フロー毎に異なる鍵の定義ができるようになるため、以降の認証、鍵交換で、このフローに関する認証、鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようにするため、複数の暗号データのやり取りが可能となる。

【0032】本発明(請求項5)に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサーバ又はクライアントとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手段を行なうコンピュータプログラム処理手段と、前記ネットワーク上におけるデータの送信時に、当該データのエンコードを行うための装置に付与されている。

14

ヤナルを介してまたは送達係員の装置が持つコンテナーを一般に識別可能な識別子を付与された形で、送達または受領するコンテナー送受積手段とを具備し、前記所定のコンテナー保護手続きに含まれる少なくとも一部の手段においてやり取りされる情報に、前記識別子を含め、前記コンテナーのやり取りを行うサービス、サブユニット、戻送コンテナもしくはアラグの識別子、または送達係員の装置が前記コンテナーを一般に識別可能な識別子を付与する少なくとも一つを付与することを得意とする。

【0030】本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグ、あるいは超子チャネルから送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能になり、もって同一ノード同士でも、同時に複数個の鍵を定義できるようなになるため、複数の暗号化データのやり取りが可能となる。あるいは、本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグ、あるいは前記特定の識別子を持って、送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【0031】本説明（請求項16）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、第1のネットワーク上の装置またはサーバまたはサブリックと、少なくとも既設手続きをおよぼすまたは鍵交換手続きを含む所定のコンテンツ保護手段と、第1のコピプロテクト処理手段と、第2のネットワーク上の装置またはサーバまたはサブリックと、少なくとも既設手続きおよび/または鍵交換手段を含む所定のコンテンツ保護手段と、第2のコピプロテクト処理手段とを備える。

テクニオン処理手段と、前記第2のインタフェース手段から呼出された特定のコンテントを含むデータを受信するコンテント受信手段と、前記第1のインタフェース手段から受信された前記受信されたデータを、前記第1のコンテントラテラル処理手段で提供されるコンテント保護用の處で復号化する復号化手段と、前記復号化されたデータを、別の符号形式に形成したデータに変換する変換手段と、前記変号化されたデータを、前記第2のコンテントラテラル処理手段で提供されるコンテント保護用の處で呼出される呼号化手段と、前記呼号化されたデータを、前記第2のインタフェース手段へ転送するコンテント送信手段とを具備したことを特徴とする。

【0033】本発明によれば、第1のネットワークを伝送させるデータが保護されるべきコンテンツであり、且つ、第1のネットワークと第2のネットワークの通信接続が著しく異なる場合のように、第2のネットワークに元のデータとは異なるデータ形式で転送することが求め

られた場合に、変換手段によってデータ形式の変換を行う。第1のネットワーク上の装置から第2のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、両区間（両データ形式）においても、不正コピー等を未然に防ぐことが可能になる。

【0036】 好ましくは、請求項16に記載の中継装置において、前記第2のネットワーク上の装置またはサーバまたはサブユニットを、自中継装置上のものとして、前記第1のネットワーク側に開示するとともに、前記第1のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサーバまたはサブユニットの情報の開示が受信された場合に、この情報に応じた内容の情報を前記第2のネットワーク上の装置またはサーバまたはサブユニット宛に送信するとともに、前記第1のネットワーク上の装置またはサーバまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に開示するとともに、前記第2のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサーバまたはサブユニットの情報の開示が受信された場合に、この情報に応じた内容の情報を前記第1のネットワーク上の装置またはサーバまたはサブユニット宛に送信する手段を更に具備し、前記代理構成手段は、前記第1または第2の一方のネットワーク上の装置と、前記第1または第2の他方のネットワーク上の装置またはサーバまたはサブユニットとの接続手段を含む所定のコンテンツ保護手続きを行う場合には、前記第1または第2の一方のコピープロテクト処理手段を用いて前記一方のネットワーク上の装置と前記所定のコンテンツ保護手続きを行うとともに、前記第1または第2の他方のコピープロテクト処理手段を用いて前記他方のネットワーク上の装置またはサーバまたはサブユニットと該所定のコンテンツ保護手続きを行うようにしてもよい。

【0038】 また、好ましくは、請求項16に記載の中継装置において、前記コンテンツ受信手段は、前記第2のコピープロテクト処理手段を用いて、前記第2のネットワーク上の装置またはサーバまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第1のコピープロテクト処理手段を用いて、前記第1のネットワーク上の装置またはサーバまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うようにしてもよい。なお、前記所定のコンテンツ保護手続きのうち少なくとも一部は、認証手続きである。このようにすれば、第2のネットワーク上の装置またはサーバまたはサブユニットが信頼に足るデバイスであるかどうかを未然に知ることができるようになり、まず第2のネットワーク上の装置等と認証手続きを行い、その後、第1のネットワーク上の装置等との認証に失敗した場合に、第1のネットワーク上の装置等との認証を改めて行わなくてもよいが、通信記録や処理資源の節約になる。

【0039】 また、本発明に係る通信装置は、第1の装置の側面に供される画面情報のためのプログラムを含む、第1の制御プログラムを受信し、これを解釈するプロセッサ手段と、このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル面とを有する。画面作成手段と、前記パネル面へのコンテンツと、前記第1の装置の側面のためのコンテンツとの対応関係を記憶する記憶手段と、前記パネル面をサブユニットとして第2の装置に公開するサブユニット処理手段と、前記サブユニットへのコンテンツを受信した場合、前記記憶手段を参照してこのコンテンツを前記第1の装置の側面のためのコンテンツに変換して、これを送出する手段とを具備したことを特徴とする。一般に、前記のような制御プログラムを解釈させるためには、仮想マシンと呼ばれる計算環境を用意する必要があるのに対し、パネル面面を通じた機器制御は、簡単なコンソール型を用意するだけでよい。また、簡単な計算環境を用意しておけばよい。本発明によれば、前記制御プログラムを持たない第2の装置に対しても、パネル面面という形で、前記第1の装置の側面インタフェースを提供することが可能になる。

【0040】 なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0041】 また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【発明の実施の形態】 以下、図面を参照しながら発明の実施の形態を説明する。

【0043】（第1の実施形態）図1は、ある家庭のホームネットワークの全体構成の一例である。

【0044】 このホームネットワークには、送信ノード101、中継ノード102、無線ノード103の3つが接続されており、送信ノード101と中継ノード102は（有線の）IEEE1394バス104に、中継ノード102と無線ノード103は無線網にそれぞれ接続されている。ただし、後述するような方法で、各ノードは互いに通信ができるようになっている。

【0045】 本実施形態では、送信ノード101から送出されたMPEG映像を、中継ノード102で中継し、無線区間を經由して無線ノード103に送信する場合を例として説明する。その際、著作権保護（不正コピーの防止）のために、送信ノード101と無線ノード103の間で転送されるMPEG映像データは暗号化される場合を考える。

【0046】 なお、図1では、3つのノードを示しているが、もちろん、これらの他にノードが接続されているもよい（後述する他の実施形態においても同様である）。

【0047】 図2に、送信ノード101の内部構造の一例を示す。

【0048】 送信ノード101は、内部にMPEG映像データを蓄積している装置であり、要求に応じてMPEG映像データをIEEE1394バス104を通じて送出する。その際、IEEE1394バス上において不正コピーをされることを未然に防止するために、必要な場合には送出するMPEG映像データを暗号化して送出する機能を持つ。そのため、MPEG映像データを受信するノードと、該データ、暗号鍵等の交換を行うための機構も持つ。

【0049】 図2に示されるように、この送信ノード101は、IEEE1394インタフェース401、AV/ビデオコルの処理を行うAV/ビデオコル処理部402、AV/ビデオコル内のコピープロテクト処理に関する処理を行うコピープロテクト処理部403、IEEE1394バスを通じて送受信されるデータのうち、同期チャネルを通してやり取りされるデータについて送受信するISO信号送受信部404、MPEG映像のストレージであるMPEGスレージ部406、コピープロテクト処理部403から暗号鍵Kをもらい、MPEG映像を暗号化してISO信号送受信部404に送出する暗号化部405を有する。ここで、コピープロテクト処理部403は、認証のためのフオーマットAcertを持つ。

【0050】 次に、図3に、中継ノード102の内部構造の一例を示す。

【0051】 中継ノード102は、IEEE1394バ

ス側から受信したデータ（MPEG映像データ）を無線区間側にフオーマットする機能の他に、IEEE1394バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してIEEE1394バス側のノード（本実施形態では送信ノード101）の代理サーバとなり、IEEE1394バス側のノードの機能を代理で提供する機能が存在する。

【0052】 図3に示されるように、この中継ノード102は、IEEE1394インタフェース201、無線インタフェース202、AV/ビデオコル処理部203、ISO信号送受信部204、無線区間の同期チャネルの信号の送受信を行う無線ISO信号送受信部205、IEEE1394バス上のノードの構成情報を収集したり、自らの構成情報（自らがどのような機能を持っているかについての情報等）をIEEE1394バス上に広告する機能を持つ1394バス構成認識部206、IEEE1394バス側に対して無線区間のノードやサーバ（サブユニット）を代理で公開したり、無線区間のノードやサーバへのコネクタ等を代理で受け付け、これを無線区間側に必要に応じてプロトコル変換をして送出したり、あるいは無線区間側に対してIEEE1394バス側のノードやサーバ（サブユニット）の代理公開やコネクタの代理受付/解放等を行う代理サーバユニット構成部207、無線区間上のノードの構成情報を収集したり、自らの構成情報（自らがどのような機能を持っているかについての情報等）を無線区間上に広告する機能を持つ無線区間構成認識部209、コピープロテクト処理に関する処理を行い、1394バスと無線区間間または無線区間と無線区間間処理に関するコピープロテクト処理部210、無線区間でやり取りされる情報を透過的にフオーマットさせるコピープロテクト前部/フオーマット部210、無線区間でやり取りされる制御パケットの送受信を行う無線ノード制御パケット送受信部211を有する。

【0053】 次に、図4に、無線ノード103の内部構造の一例を示す。

【0054】 無線区間においていわゆるIEEE1394プロトコル（物理レイヤプロトコル、リンクレイヤプロトコル等）が稼働している必要は必ずしもなく、IEEE802.11や無線LAN等、任意の無線プロトコルを利用することを規定するが、本実施形態では、特に、いわゆるQOS機能（同相通信機能）を有する無線網であることを規定する。ただし、本実施形態は、無線区間部分にQOS機能が求められると前提されるものではない。

【0055】 いわゆるIEEE1394ノードではない無線ノード103が、IEEE1394バスに繋がれたノード（本実施形態では送信ノード101）と通信を行うために、前述のように、中継ノード102がIEEE1394バス上のノードや機能（サブユニット）をエ

23

ノート10.2から到達したものである。ここで、それは誤解であるが、この時点で無線ノート10.3は、この町を解くための鍵を有している(もしくはその鍵を生産できる)ための元となるデータがない)ため、この状態では町を解いて、MPEC映像を取り出すことはできない。ここで、無線ノート10.3は隠匿手書きがMPEC映像の近百年と必要であることを示唆する。

【0083】そこで、無線ノード103のコピータロ
テション処理部303は、読取要求を暗号化データ
の送信元に対して送信する。先に述べたように、無線ノ
ード103には、上記暗号化データを送信する中継ノ
ード102（内の、サブユニット部）は映像送信サブユニ
ット102（内の、サブユニットID=b（b=0とする
）、サブユニット）であるように認識されている。

【0008】また、図5のSS52.1のように、中継ノード102に対して、「無線ノードにおいて、無線同次サネルキヤを受信しているのは、サブエニット種別=MEGテラノード/チクスノビノサエニットで、かつ、サブエニットID=c(c=0と5)の、サブエニットである。無線同次サネルキヤに直交化チータを送信しているのはどのサブエニットか」という意味合いの問い合わせを送信してもよい、これにより、中継ノード102は、「無線同次サネルキヤに送信しているのは、映像送信サブエニットのサブエニットID=0である。」との返答を返す(サブエニット552.2, S731, S831)。これにより、無線ノード103は、認証を行なう前が中継ノードの映像送信サブエニットであることを認識できる。

【0085】このように、認証要求の発生を認識し、中継ノード102の映像送信サブユニットのサブユニットID=0)に対し、認証要求を送信する。この送信の方法として、認証要求パケットの宛先を「中継ノードの映像送信サブユニット(のサブユニットID=0)」としてもよいし、認証要求パケットの任意の位置に「映像送信サブユニット(のサブユニットID=0)」という情報を入れ、認証要求は映像送信サブユニットのサブユニットID=0)であると言うことを明確に表示してもよい。前者の場合は、中継ノードの各サブユニット内に認証・鍵交換の手続きがなされていることを意味する。後者の場合は、中継ノードのある特定の処理部が、一括して、各サブユニットの認証・鍵交換を行なうことを意味する。

【0080】その際、認証要求には、無納ノード103の認証ノードアベリBcertを付与する。(ステップ804、S508)。Bcertは、無納ノード103のMPEGデコード/デマルチプレクサユニットの認証ノードアベリであったもよい。なお、コピーガードシフト処理部は、サブユニット毎(サブユニット組別毎)でなく、サブユニットID毎に認証ノードアベリを用いてもよい。

24

【0087】認証要求を受信（ステップS710）した中継ノードは、代理型ノード208を参照して、この認証要求の要求先が実は送信ノード101（の映像送信ソフトウェア）のソフトウェアID=a（a=0とする）であることを認識する。

【0080】中継ノード102は、送信ノード101に対して、中継ノードにおいて、両サテライトxを受信しているのは MPEG デコーダ/エンコーサがアノニミットのサフェニットID=0である、両サテライトxに符号化データを送信しているのは、送信ノードのどちらにサフェニットか? という意味合いの問合わせを送信してよい (ステツプS523、S631、S732)。

2. これに対し、送信ノード101は、「両サテライトxにxに送信しているのは、映像送信のサフェニットID=0である、」との返答を返す (ステツプS624、S631、S732)。

〔0089〕このようにして、認識要求や指示を認識し、たとえば、ステツプ5508にて受領した認識要求を、中身を変えずに (Beceit等はそのまま現して) 送信ノート1011に封じ付けたステツプ5509、5711)。すなわち、最先アドレス、認識要求の宛先であるサブユニット以外の認識ノート等は、中継ノートは自動的に転送できる。

【0090】認証要求の転送の際は、先に拒却したように、認証要求パケットの宛先を映像送信サブユニット（のサブユニットID=0）としてもよいし、認証要求パケットの任意の位置に当該サブユニットを明示する情報を入れ、認証要求先は当該サブユニットであると言うことを明確に表示してもよい。

【0099】ここで、認証要求の中央をなすプロトタイプすること、この認証要求はその中央をなすプロトタイプ1011に到達することになり、結局、送信プロトタイプ101と無線プロトタイプ103との間で、実際の認証手続きは進んでいくことになり、しかも無線プロトタイプ102をはじめ、その他のノードにはその認証が説明されないような幾分曖昧な情報が知られることなく、以上の手続きを行っていくことが可能である。

【009】認証要求を受け取った通信ノード101は、これを中継ノード102のMPEGデコーダ/デマルチプラキユニットから送られた認証要求である（ステップ7604）、その後、Bcetriと照合する（ステップ7604）、その後、Bcetriから無線ノード103のMPEGデコーダ/デマルチプラキユニットを特定できるID（Bd1d）を抽出し（ステップ7605）、これとともに、やはり同様の認証要求を認証要求の送信元に対して行かせる。ただし、送信ノード101は、Bcetriが無線ノード103の認証ソフトウェアであるとは認識することなく、むしろ中継ノード102（のMPEGデコーダ/デマルチプラキユニット）の認証ソフトウェアであるとは認識している。

(14) 特開2000-174797

25

【0093】この拡張要求には、送信ノード101 (の映像送出用サブユニット) の拡張フォーマットparameterと、Bd1dが含まれる。ここで、送信ノード101とは、該拡張要求 (スロット750) の送信元中継局である。該拡張要求 (スロット750) の送信元サブユニット102 (のMPEGデコード/デマルチプレクサユニット) であると同解釈しているため、この拡張要求の送信先はやはり中継ノード102となる (スロット5600、6, 5510)。

【00941】これを受領(スチブツS712)した中継機ポート102は、代理ケーブル208を参照して、このポート102は、要求先が無線ポート103 (MPPE、G3ポート/デススススス機能) であることを認識し、このまま接続要求を、中継機を変えて(Accept等は)この要求を預けて 無線ポート103に対してアワードポートする(スチブツS511, S713)。この接続要求の送信元は中継ポート102である。

10095] これを受け取った無線ノード103は、これら中継ノード102の映像送信サブユニットから送られてきた認証要求と相対する(ステップS805)。その後、Acerが送信ノード101の映像送信サブユニットを特定できるID (Ad1d) を抽出し、認証鍵の交換に必要な預りの手続きを、認証要求の送信元に対して行うとする。なお、この場合も、無線ノード103は、Acerが送信ノード101の認証ノード103であるとは意識せず、むしろ中継ノード102(の映像送信サブユニット)の認証ノードとして意識する。

【0099】この認証鍵の交換に必要なのは手続きとして、無効ノード103は、認証要求の送信元（この無効ノードが所属しているノード）に対して認証・鍵交換手続のバケットを送信する（ステップS112）。この認証・鍵交換手続きバケットには、鍵交換初期値、署名、Acceitの中に含まれていた送信ノード（この映像送信サブユニット）のデバイスID（Adid）等が含まれている（ステップS806）。ここで、無効ノード103は、映像送信要求（ステップS511）の送信元は中継ノード102（この映像送信サブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード102となる。

「0099」これを受信した中継ノード102は、代理
 テーブル208を参照して、この送信手続きの本来の受
 取先が送信ノード101（この映像送信サブユニット）で
 あることを認識し、この送信手続きをサブユニットを
 要えずに送信ノード101に対してフックアップする。中
 継ノード5513、5714）。このパケットの送信元は
 中継ノード102である。

【0098】これと同様の手振きが送信ノード101→中継ノード102→無線ノード103の方向に対しても行われる(ステップS514、S515、S609、S715、S807)。

26

【0099】この認証手段は、パスワードを受信した送信ノード101および無線ノード103は、それぞれ、受信したパスワードが改ざんされていなければ、受信したパスワードが改ざんされてきた認証ソフトウェアで正しいものであるかどうかの確認等を行い、与えられた値を保持して共通の認証鍵Kauthを導き出す。この共通の認証鍵Kauthは、送信ノードの映像送信ソフトウェア（機能）と無線ノードのMPEGデコーダソフトウェア（機能）との間で共通に持つことで、この鍵Kauthを、この両者（送信ノード101、無線ノード103）以外の他人に知られることなく共有することから、特許でできるようになる（ソフトウェア607、ソフトウェア608、S808）。

【0100】この認証鍵Kauthを使って、装置にMESSAGEの暗号化を行うコンテントキーの計算ができるようになる。具体的な手順はここでは省略するが、送信ポート101から無線LANポート2に、IEEE1394のコピーフロッピー方式(6C方式)のように、交換線やケーブル(図)の線を別途送ることににより、コンテントキーKの計算ができるようになっていともよい(STEP518, STEP519)。

[0101]さて、このようにして、送信ノード101 (の映像送信サブユニット)と無線ノード103 (のMPEGデコード/デマルチプレクシング)との間で、コンテンツキーKの値が共有できるようになった。

【0102】ここで、送信ノード101が、送信するMPEG映像を、コドンエラー率を使って、符号化部405に送付する(ステップS610)。これを1394バスの間隔チャネル々々を置いて(中継ノード102)のMPEGデコード/デマシレイザサブユニット)に対して送信する(ステップS616、S611)。

ら同間チャネル#xを通して送られてくる符号化された MPEG映像を、ISO信号送受信部204から無線1SO信号送受信部205を通して、無線同間チャネル#yに送信する(ステップS517、S716)。

10 [0104] これを受けて、本発明のモード103は、キークの値を使ってMPEと映像化の値を復号化する(ステップ809、ステップ810)。復号化されたMPEはGデータは、MPEGデータ部306にて復号化された(ステップ811)、これをデコスプレ部307にて再生成表示する(ステップ812)。

に代理ノードが存在するよう相互接続の環境において
[0105] このように、1394バスと無線網との間
も、エンブノードの同一同士（本実施形態では送信
ノード101と無線ノード103）が電圧手続きや通信
握手を行うことができ、さらにその内容を中継ノ
ード102を含め、その他のノードが知ることができ
ない仕組みとなっている。また、実際のMPEG映像等のコ
ンテンツ保護に必要なデータの転送も、コピーが不可

なように情報の全てで暗号化されており、安全なデータ伝送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ伝送を行うことが可能になる。

[0106] なお、以上の実施形態は、認証手続きや、暗号鍵の交換手続き等、ノードのサブユニット単位で行ってきたが、無線ノード単位でこれを行うことも可能である。なお、ノード単位で行う例については、次の第2の実施形態で説明するので、例えばこれを適用すればよい。

[0107] また、以上の実施形態では、認証および鍵交換のための手続きを暗号化データの受取後に行ってきたが、相手機では、暗号化データ受信に先だって行ってもらう構成もない。例えば、装置や装置がアドレス情報の立ち上げ時に相手機の手続きを行ってもよい。

[0108] (第2の実施形態) 次に、第2の実施形態について説明する。

[0109] 第1の実施形態では、送信ノードと無線ノードとが、直接、互いに認証手続きや鍵交換手続きを行ってきた。すなわち、送信ノード (の映像サブユニット) と無線ノード (のMPEGデコーダ/デマルチプレクサ) とが、直接、互いに認証し、暗号鍵の交換手続きを行った。暗号化データのやり取りを行ってきた。この際、中継ノードは、送信ノードに対しては無線ノードのMPEGデコーダ/デマルチプレクサ機能の代理機能を実現し、無線ノードに対しては送信ノードの映像サブユニットの代理機能を実現してきたが、上記の認証手続きおよび暗号化データのやり取りの部分については、これらのデータのやり取りの部分を、代理していたサブユニットなり機能なりに行う形であった。

[0110] これに対し、第2の実施形態では、中継ノードにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを継続する場合の例を示す。すなわち、送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間で、各々のコピープロテクション手続きは同じである。つまり、この実施形態においても、中継ノードは、送信ノードあるいは無線ノードに対して代理サービスを提供するものの、コピープロテクションについては、中継ノード自身が認証ソフトウェアを持ち、中継ノード自身が、1394バス区間のMPEGデータの暗号化伝送についての責任を負担するとともに、無線区間のMPEGデータの暗号化伝送についての責任を負担する場合の例である。

[0111] 図20に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的に第1の実施形態と同様である。

[0112] 図21に、送信ノード2101の内部構造の一例を示す。これも第1の実施形態と基本的に同様である。

[0113] 次に、図22に、中継ノード2102の内

部構造の一例を示す。

[0114] 中継ノード2102は、第1の実施形態と同様に、IEEE1394バス側のノードに対して無線ノードの代理サービスとなり、無線ノードの機能を代理で提供する場合、および無線区間のノードに対してIEEE1394バス側のノード (本実施形態では送信ノード2101) の代理サービスとなり、IEEE1394バス側のノードの機能を代理で提供する場合を持つ。

[0115] また、IEEE1394バス側から受信したデータ (MPEG映像データ) を無線区間側にサブユニットとする機能を持つが、第1の実施形態と相違する点は、認証データや暗号化データ、コピープロテクションに関する手続きがIEEE1394バス側と無線区間との両方について、この中継ノード2102において数値化されており、IEEE1394バス側については認証ソフトウェアBcCerをIEEE1394コピープロテクション処理部2208に、無線区間側については認証ソフトウェアCcCerを無線区間コピープロテクション処理部2212にそれぞれ持ち、1394バスの両側でやり取りから入力されてきた暗号化データについては、ISO信号受信部2203にて受信暗号復号化部2204にて暗号復号化一度号化されたMPEG映像を、暗号化部2205にて暗号化暗号化無線ISO信号送受信部2206にて、無線同期信号上に送信、というプロセスを繰り返す。

[0116] これらの認証ソフトウェアは、IEEE1394バスサブユニット等、あるいは無線区間サブユニットに一つずつ、サブユニット毎 (サブユニット別) に一つずつ持っていてよい。

[0117] ここで、AcCerとBcCerは、同じ認証機能 (例えばIEEE1394のコピープロテクションを担当する認証機能) が実行した認証ソフトウェアであると仮定するが、後述する無線区間の認証ソフトウェア (後述するCcCerとDcCer) については、同じくこの認証機能が実行したものであってもよい。無線区間を担当する別の認証機能が実行する認証ソフトウェアであってもよい。

[0118] 次に、図23に、無線ノード2103の内部構造の一例を示す。コピープロテクション処理部2303が、無線区間向けの認証ソフトウェアDcCerを持っていて、これは、基本的に第1の実施形態の無線ノードと同様である。

[0119] 次に、実際のコピープロテクションを施した上でMPEG映像全体のシーケンスについて、図24/図25 (全体のシーケンス例)、図26/図27 (送信ノード2101のフローチャート例)、図28/図29/図30/図31 (中継ノード2102のフローチャート例)、図32/図33 (無線ノード2103のフローチャート例) を参照しながら説明する。

[0120] まず、無線ノード2103は、自分の構成情報を中継ノード2102に通知する (ステップS2501)。構成情報は、自分 (無線ノード) がMPEGデコード/デマルチプレクサ機能を持つこと、暗号化のための認証ソフトウェアを持っていることなどである (図14参照)。ここで、認証のための認証ソフトウェアが、無線区間の認証ソフトウェアである旨を通知してもよい (ステップS2801)。

[0121] これを受信した中継ノード2102は、無線ノード2101が認証ソフトウェアを持つことや、MPEGデコード/デマルチプレクサ機能を持つことを確認する (ステップS2701)。中継ノード2102は、第1の実施形態と同様に、このMPEGデコード/デマルチプレクサ機能、IEEE1212レシタやAV/Cプロトコル等を使って、中継ノード2102自身のサブユニットとしてIEEE1394バス側に広告する (ステップS2502)。

[0122] そのため、中継ノード2102は、代理サブユニット構成部2210内に代理サブユニット2214を持つ。この代理サブユニット2214は、基本的に第1の実施形態と同様であり、図34/図35のように、中継ノード2102が代理で広告している形と、その媒体との対応付けが記されているテーブルである。

[0123] ここで、図34のように、無線ノード2103のMPEGデコード/デマルチプレクサ機能が、中継ノード自身のサブユニットとして代理広告される (ステップS2702、S2703)。

[0124] そのため、送信ノード2101から見た中継ノード2102の構成は、図36のように見えることになる (ステップS2601)。

[0125] 以上は、IEEE1394バス側について説明であったが、第1の実施形態と同様に、これと同様の関係が無線区間でも成り立っている。すなわち、中継ノード2102は、IEEE1394バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスは無線区間側に行っている。よって、図35のような設定がなされ、無線ノードから見た中継ノード2102の構成は図37のように見える。

[0126] さて、中継ノード2102内にMPEGデコード/デマルチプレクサユニットがあると認識した送信ノード2101は、このサブユニットに対して、MPEG映像を伝送することを目的に、1394バス上に同期チャネル#xを確立し、AV/Cプロトコルにてこの同期チャネル#x (を受信するサブユニット) と、MPEGデコード/デマルチプレクサユニットとを接続し、映像を表示し、この命令を出す (ステップS2503、S2602)。送信ノード2101は、このサブユニットが中継ノード2102にあるものと解釈しているため、命令の送信先は中継ノード2102である。

[0127] これを受信 (ステップS2704) した中

継ノード2102は、受信した命令パケットを解釈し、その命令が自分が代理サービスを行っているMPEGデコード/デマルチプレクサユニットに対する命令であることを認識し、代理サブユニット2210を参照して、この命令先の本体は無線ノード2103にあることを認識する (ステップS2705)。

[0128] ここで、図20の無線区間は、QOS対応の無線LANになっており、予め定められた手順を踏めば、パケット遅延や遅延等の品質劣化無く、転送データを送信先まで伝送することが可能であるとする。この無線LAN上では、データは図38のように、イーサネットフレームと同様のフレーム、すなわち「送信元アドレス、宛先アドレス、データ」のようパケットを持つ。無線フレームで転送される。

[0129] さて、IEEE1394バス同期チャネル#xを通して受信したデータを、無線ノード側にフォーワードすべく、無線区間のQOS設定を行う。さらにISO信号送受信部2203 (同期チャネル#xを受信) と無線ISO信号送受信部2206 (QOS保証を行なう無線フレームにて送信) を図22の点線のように接続し (まだ暗号の復号化ができていないため)、1394バスサブユニット2201から入力されたISO入力データを無線区間のそのまのソフトウェアで転送するように (ステップS2504、S2706、S2707)。

[0130] さらに、無線ノード2103に対して、上記無線フレームを通して、データを転送するので、これを受信し、その結果をデマルチプレクサに指示し、この命令を無線ノード制御パケットの形で送信する (ステップS2505、S2708、S2802)。この制御パケットは、IEEE1394AV/Cプロトコル、あるいはIEC61883プロトコル、これらの変形したものを用いてもよい。後述するように、本実施形態では、無線LAN上に同期チャネルの概念はないものの、転送するデータにSID (SID) なる領域を設け、無線区間にQOSデータを一旦に区別できるように、転送しているQOSデータを一旦に区別できるようにしており、このSIDの値をIEEE1394の同期チャネルのように、データフローの別別に用いることができる。無線ノード制御パケットの一例を図39に示す。パケットの送信元は中継ノード2102である。

[0131] これを受信した無線ノード2103は、αなるSSIDが付与されて、データがQOS伝送されることが認識する。

[0132] この後、送信ノード2101は、同期チャネル#xを通して、暗号化されたMPEG映像を伝送する (ステップS2506、S2603)。コドンツはK1とする。この暗号鍵は、後述する交換鍵やサブユニットの暗号として輸出される。

[0133] また、この暗号化されたMPEG映像を送信するフレームには、同期チャネル番号の他、送信ノ

31

ドを識別する「送信ノードID」が含まれていてもよい。

[0134] これを受信した中継ノード2102は、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信ノードID」を参照して、このデータを送信しているが送信ノード2101であることを認識し（スレッツS2709）、送信ノード2101に対して、「同期チャネル#x」を送信して、このデータを送信しているのは、送信ノード2101のどのサブユニットかを確かめるため、認証先の問合せを行なう（スレッツS2507、S2710）。この際、データが伝送されている同期チャネル番号（#x）を記載して、送信ノード2101が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する自身のサブユニット（本実施形態の場合、中継ノード2102のMPEGデコード/デアスプレイサブユニットのサブユニットID=0）も通知する。これは、送信ノード2101から見た認証先を通知する役割を持つ。

[0135] なお、この認証先問合せをバケットと、後述する認証先既客バケットは、認証機関のプラグイン機能でハッシュや暗号化したデータを鍵子型として処理しておき、改ざん等が無いことを確認できるようにしてもよい。

[0136] さて、認証先問合せを受信（スレッツS2604）した送信ノード2101は、同期チャネル#xに対して送信しているデータを受信しているサブユニットが、中継ノード2102のMPEGデコード/デアスプレイサブユニットであることを認識するとともに、自らが従前同期チャネル#xに送信しているサブユニットが、映像送信サブユニット（サブユニットID=0）であることを、認証先既客バケットとして、中継ノード2102に通知する（スレッツS2508、S2605）。

[0137] これにより、中継ノード2102は、同期チャネル#xにデータを送信しているサブユニットが、送信ノード2101の映像送信サブユニット（サブユニットID=0）であることを認識できる（スレッツS2711）。

[0138] 同期チャネル#xにデータを送信しているサブユニットが、送信ノード2101の映像送信サブユニットであることを認識した中継ノード2102（のMPEGデコード/デアスプレイサブユニットの代理機能）は、続いて送信ノード2101の映像送信サブユニットに対して認証要求を行なう。この認証要求には、中継ノード、あるいは中継ノードのMPEGデコード/デアスプレイサブユニットの認証ソフトウェア（Bcert1）が共に伝送される（スレッツS2509、S2606、S2607、S2712）。この認証要求と認証ソフトウェアの交換は、第1の実施形態と同様に、送信ノ

32

ード2101（の映像送信サブユニット）から中継ノード2102（のMPEGデコード/デアスプレイサブユニット）に向けても行われる（スレッツS2510、S2608、S2713、S2714）。このように、第2の実施形態においても、認証・鍵交換はサブユニットに関する情報も交換するのは、同じ実施例上の通信でも、通信しているサブユニットが異なれば、異なる鍵の使用ができるようにするためである。

[0139] お互いに認証が完了した両ノードは、第1の実施形態と同様に認証・鍵交換手続きを行い（スレッツS2511、S25112、S2609、S2715）、認証鍵Kauthを共有する。この認証鍵を使って、送信ノード2101は、交換鍵やサブノードの伝送を中継ノード2102に対して行ない（スレッツS2512、S2610、S2716）、結局、中継ノード2102では、コンテンツ鍵K1の値を知ることができるようになる（スレッツS2717）。

[0140] 以降、伝送されてくるコンテンツ鍵K1で暗号化されたMPEG映像（同期チャネル#x経由）（スレッツS2513、S2611、S2612）は、中継ノード2102にて復号化され（スレッツS2514、S2718）、さらに無線区間内に別に用意されたコンテンツ鍵K2で再暗号化され（スレッツS2515、S2616、S2719）、無線区間上をQOSが保証される形で、無線ノード2103に対して伝送される（スレッツS2517、S2720、S2803）。この時点では、MPEG映像はISO恒時送受信部2203、暗号復号化部2204、暗号化部2205、無線ISO恒時送受信部2206というバスを通る。

[0141] 先に述べたように、このとき中継ノード2102が、無線区間内に送信しているデータの区別ができるようにするために、SID=αなる、中継ノード2102で一意な値を付与して送出してもよい。ここでは、この一意な値をαとする。すなわち、αの値のついたデータは、IEEE1394の同期チャネル#xから受信したデータ（をコンテンツ鍵K1で復号化し、コンテンツ鍵K2で再暗号化したもの）である。中継ノード2102は、αのSIDを付けて無線区間に送出しているデータは、自身の無線区間側の映像送信サブユニットの代理機能から送信しているデータであることを認識している。

[0142] これを受信した無線ノード2103の動作は、基本的に既に説明した、暗号化データを受信した中継ノード2102の動作と同様である。すなわち、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信ノードID」を参照して、このデータを送信しているが中継ノード2102であることを認識し、中継ノード2102に対して、「αなる値を付与して、このデータを送信しているのは、中継ノード2102のどのサブユニットかを確かめるた

33

め、中継ノードに認証先の問合せを行なう（スレッツS2518、S2804）。

[0143] この際、データが伝送されているSIDの値（α）を記載して、中継ノード2102が、データを通信しているサブユニットを特定できるようにしておくとともに、このデータを受信する受信側のサブユニット（本実施形態の場合、無線ノード2103のMPEGデコード/デアスプレイサブユニットのサブユニットID=0）も通知する。これは、中継ノード2102から見た認証先を通知する役割を持つ。

[0144] 認証先問合せを受信（スレッツS2721）した中継ノード2102は、SID=αに対して送信しているデータを受信しているサブユニットが、無線ノード2103のMPEGデコード/デアスプレイサブユニット（サブユニットID=0）であることを認識するとともに、自らがSID=αを付与して送信しているサブユニットが、映像送信サブユニットであることを、認証先既客バケットとして、無線ノード2103に通知する（スレッツS2519、S2722、S2805）。

[0145] これにより、無線ノード2103は、SID=αを付与してデータを送信しているサブユニットが、中継ノード2102の映像送信サブユニットであることを認識し（無線ノード2103（のMPEGデコード/デアスプレイサブユニット）は、続いて送信要求を行なう（スレッツS2520、S2723、S2724、S2806）。この認証要求には、無線ノード（または無線ノードのMPEGデコード/デアスプレイサブユニット）の認証ソフトウェア（Decert1）が共に伝送される。この認証要求と認証ソフトウェアの交換は、中継ノード2102（の映像送信サブユニット）から無線ノード2103（のMPEGデコード/デアスプレイサブユニット）に向けても行われる（スレッツS2521、S2725、S2807）。

[0147] お互いに認証が完了した両ノードは、続いて認証・鍵交換手続きを行い（スレッツS2522、S2523、S2726、S2808）、認証鍵Kauthと共有する。この認証鍵を使って、中継ノード2102は、交換鍵やサブノードの伝送を無線ノード2103に対して行ない（スレッツS2624、S2727、S2809）、結局、無線ノード2103で、コンテンツ鍵K2の値を知ることができるようになる（スレッツS2810）。

[0148] なお、これまでの説明では送信ノードと中継ノード間の認証・鍵交換と、中継ノードと無線ノード間の認証・鍵交換とは、順次行われる形で説明したが、

34

逆の順番でもよいし、両者を並行して行うことも可能である。

[0149] 以降、伝送されてくるコンテンツ鍵K1で暗号化されたMPEG映像（スレッツS2525）は、中継ノード2102にて復号化され（スレッツS2526）、さらに無線区間内に別に用意されたコンテンツ鍵K2で再暗号化され（スレッツS2527、S2528、S2728）、無線区間上をQOSが保証される形で、SID=αが付与された無線ノードの形で無線ノード2103に対して伝送される（スレッツS2529、S2729）。

[0150] 今回は、無線ノード2103は、先に入手した交換鍵、サブノードの値を使って、コンテンツ鍵K2を計算できるので、これを復号化することが可能であり（スレッツS2530、S2811）、これをデアスプレイ部2307にて再生する（スレッツS2812）。

[0151] このように、IEEE1394バスと無線網の間に代理ノードが存在するような相互接続の環境においても、代理機能を提供する中継ノードと送信ノード、および中継ノードと受信ノードが、それぞれの区間で、認証手続きや鍵交換手続きを行うことで、実際のMPEG映像等のコンテンツ保護の必要なデータの伝送を、コピーが不可能なように接続の全てで暗号化して行うことができ、安全なデータ伝送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ伝送が可能になる。

[0152] もちろん、中継ノード2102の「生のMPEGデータ」が流れる部分、具体的には暗号復号化部2204と暗号化部2205との間には、データコピーを許容する危険が考えられるため、この部分でデータコピーがなされないようにするための工夫（例えば、暗号復号化部と暗号化部を一体のLSIにするなど）がなされていると、この間でのフローをあてるとしてデータを盗聴（不正コピー）することが実質的に不可能になるため、このような対策を行っておくことが有益である。

[0153]（第3の実施形態）次に、第3の実施形態について説明する。

[0154] 第3の実施形態では、IEEE1394上において、HAVI規格（Specification of the Home Audio/Video Interoperability (HAVI) Architecture）等に代表される、AV/Cの上位レイヤに相当するAV機器制御ソフトウェアが稼働している場合における実施形態である。

[0155] 図40に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的に第1の実施形態と同様である。

[0156] 図41に、送信ノード4101の内部構造の一例を示す。これも第1の実施形態の場合とはほぼ同

であるが、IEEE1212レジスタ4407を演算のため、追加記述している。IEEE1212レジスタ4407には、送信ノード4101の属性、例えば「どのベンダの製品かを示す情報、例えばVTRやチューナ等といったようなエンタの製品かを示す情報、製造番号、制御ソフトウェアのバージョン、制御アイコン、コマンド等」等の情報が含まれる。

[0157]次に、図42に、中継ノード4102の内部構造の一例を示す。中継ノード4102も、第1の実施形態とほぼ同様の構成であるが、本実施形態のシーケンスを説明する際に必要なIEEE1212レジスタ4213を1394バス構成部4206内に特に記した点と、HAV1処理部4212を持つ点が第1の実施形態と異なる。HAV1処理部4212には、いわゆるHAV1パイプラインの処理を行う仮想マシン（VM）が存在する。また、本実施形態においては、制御面側の記述を行う「パナールサブユニット」の代理機能を代理サブユニット構成部4207が持つ。

[0158]次に、図43に、無線ノード4103の内部構造の一例を示す。これについても、第1の実施形態の場合と基本例には同様である。

[0159]次に、HAV1環境における、実際のコーデック動作を施した上でMPEG映像全体のシーケンスについて、図44/図45（全体のシーケンス例）、図46/図47（送信ノード4101のフローチャート例）、図48/図49/図50（中継ノード4102のフローチャート例）、図51/図52（無線ノード4103のフローチャート例）を参照しながら説明する。

[0160]まず、無線ノード4103は、自分の構成情報を中継ノード4102に通知する（ステップS4501）。このとき、これらの構成情報は、IEEE1212レジスタ形式の信号として中継ノード4102に送付するものとする。すなわち、中継ノード4102が、無線ノード4103に対して「IEEE1212で規定されるCSR（コントロール・ステータスレジスタ）空間」の、このアドレスに相当する部分についての情報を要求し、これに無線ノード4103が答える形でこのやり取りが行われてもよい。ここで、前述のように、この構成情報には、自分（無線ノード）がMPEGデコーダ/デマルチプレクサ機能を持つといったことや、認証のための認証ソフトウェアを持っていること、等が含まれる。ここで、無線ノード4103が持っている認証ソフトウェアをBecertとする。

[0161]これを受信した中継ノード4102は、無線ノード4101が認証ソフトウェアを持つことや、MPEGデコーダ/デマルチプレクサ機能を持つことを確認する（ステップS4701）。中継ノード4102は、無線ノード4101がMPEGデコーダ/デマルチプレクサ機能を持っていることをIEEE1394バス側の

ノードに対して知らせるため、このMPEGデコーダ/デマルチプレクサ機能、中継ノード4102自身のサブユニットとしてIEEE1394バス側に広告する（ステップS4502）。具体的には、自身のIEEE1212レジスタに「自分はMPEGデコーダ/デマルチプレクサ機能を持つ」旨を記載したり、AV/CFプロトコルでサブユニット機能の問い合わせを受けた場合に、自分MPEGデコーダ/デマルチプレクサユニットを持っているという形で応答を送ったりする（これにより、送信ノード4101等のIEEE1394バスに接続されたノードは、中継ノードにこの機能が存在すると認識することになる）。

[0162]そのために、中継ノード4102は、代理デコーダ208を持つ。代理デコーダ208は、図53/図54のように、中継ノード4102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

[0163]ここでは、図53のように、無線ノード4103のMPEGデコーダ/デマルチプレクサ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS4702、S4703）。

[0164]以上と逆の手続きがIEEE1394バス4104上の送信ノード4101の代理装置を無線区間側に対してみせる形で行われる（ステップS4504、S4504）。すなわち、送信ノード4101のIEEE1212レジスタ4407に、自分が映像送信機能を持つこと、およびパナール機能（制御面側機能）を持つことを記述しておき、これを中継ノード4102が読み込む（ステップS4601、S4704）。この送信ノード4101の機能を、中継ノード4102の機能として、代理して無線区間側のIEEE1212相当機能（無線区間側のCSR空間）に反映し、無線ノード4103側には、上記映像送信機能、およびパナール機能が中継ノード4102の機能であるものとして認識してもらう。この対応関係を、代理デコーダ208に図54のように反映する（ステップS4705）。

[0165]このようにして代理デコーダ208は、図53/図54のように構成される。また、送信ノード4101から見た中継ノード4102の内部構造を図55に、無線ノード4103から見た中継ノード4102の内部構造を図56に、それぞれ示す。

[0166]なお、この時点で、ステップS4503の送信ノード構成情報の中に、送信ノード4101を制御するためのHAV1のパイプラインが記されており、中継ノード4102は送信ノード4101の代理サブ、すなわちDCM（デパナールコントロールモジュール）の機能を有しているもよい。この場合、このパイプラインは、中継ノード4102のHAV1処理部4212内の仮想マシン上で稼動することになる。

[0167]さて、中継ノード4102にパナール機能が

あるものと認識した無線ノード4103は、中継ノード4102の（パナールサブユニット）に対して、パナールの表示領域コンテキストを送出する（ステップS4505、S4802）。これを受信（ステップS4706）した中継ノード4102は、代理デコーダ208を参照し、このパナール機能の実体が送信ノード4101に存在していることを認識し、前記パナール表示要求コンテキストを送信ノード4101に対してサブワードする（ステップS4506、S4707）。

[0168]これを受信（ステップS4601）した送信ノード4101は、AV/CFプロトコルにてパナール応答（つまり、制御面側の送信）を行う。送信先は、中継ノード4102である（ステップS4603、S4507）。これを受信（ステップS4708）した中継ノード4102は、代理デコーダ208を参照して、これを無線ノード4103にサブワードする（ステップS4709、S4508、S4803）。

[0169]ここで、図57に、無線ノード4103に送られてきた制御面側の一例を示す。この制御面（パナール）では、6つの表のタイトルを表示したボタンが提供される。これらのボタンは、例えば「ボタン1」、「ボタン2」、「等の名前が付けられており、ユーザがあるボタンを押すと、例えば「ボタン1」が押されたまじ」というコンテキストの形で、パナールの送信元に送られる仕組みとなっているものとする。

[0170]さて、無線ノード4103は、中継ノード4102が提供しているものと認識している映像送信サービスを受けようと考え（実際に提供しているのは送信ノード4101）、無線ノード制御パケットを使って（ステップS4509）、映像を送るための無線同期チャネル#xを確保し、このチャネルを中継ノード4102の映像送信サブユニットに接続するためのコンテキストを中継ノード4102に対して送付する（ステップS4804）。

これを受信した中継ノード4102は、代理デコーダ208を参照して、実際にこのAV/CFコンテキストが実行されるべきノード（送信ノード4191）を識別し、IEEE1394バス上に必要な帯域を確保するとともに（同期チャネル#x）、内部のISO信号送受信部4204を設定して、IEEE1394バスの同期チャネル#xと無線同期チャネル#xとを相互に接続する（ステップS4710、S4711、S4712、S4510）。また、中継ノード4102は、送信ノード4101に対し、同期チャネル#xを映像送信サブユニットに接続するコンテキストを送付する（ステップS4511、S4713）。これを受信（ステップS4604）した送信ノード4101は、映像送信サブユニットの実体である内部の映像ストリームの流れのバス（図41で2番印刷になっている部分）をIEEE1394バスの同期チャネル#xに接続する。

[0171]これと前後して、無線ノード4103のユ

ーザは、見た映像を選択するために図57のパナールの中から適当な番組を選択すべく、制御面側のボタンを押す（例えば、マウスを使ってクリックする、ペン入力する、タッチする、など）。この操作は、中継ノード4102に伝達され、これは代理デコーダ208の参照を経て送信ノード4101へのコンテキストに変換される（ステップS4805、S4714、S4715、S4605、S4512、S4513）。

[0172]この後、送信ノード4101は、同期チャネル#xを通して、暗号化されたMPEG映像を送信する（ステップS4514、S4606）。これは、中継ノード4102にて中継され、無線ノード4103に到達する（ステップS4716）。

[0173]後の手続きは、第1の実施形態の場合と同様であり、暗号化されたMPEG映像が無線ノード4103に到達する（ステップS4806）が、この時点で無線ノード4103はこの暗号を解くための鍵を有していないため、MPEG映像の送信元と認証手続きを開始する。認証手続き以降の手続きについては第1の実施形態と同様であるので、ここでの詳細な説明は省略する。

[0174]なお、第1の実施形態に比べ、認証は送信ノード4101の映像送信サブユニットに相当する機能と、無線ノードの映像受信サブユニットに相当する機能との間で実行されると考えられるが、第3の実施形態の場合には、このような認証方式の他に、送信ノード4101のパナールサブユニットが認証の対象となるような方式も考えられる。この場合は、送信ノード4101のパナールにデパナールIDが割り当てられることとなる。

[0175]なお、HAV1においては、送信ノード4101から送られてきたパイプラインであるDCM域の中に、送信ノード4101を制御するための制御面側情報が含まれる場合がある。このようなモジュールをDDI（デパナールインターフェース）と呼び、このようなモジュールは、例えば中継ノード4102内のHAV1処理部4212にて展開され、制御面側が生成される。本実施形態では、この制御面側（あるいは、それと同様の機能を持つ制御面側）を無線ノード側に見せることを考える必要があるが、この場合は、代理サブユニット構成部4207が、このDDIに含まれる画面構成情報を認識して（例えば、画面構成のためのシステムコールをイベントとして認識して、生成される最終画面の概要を推察する方法や、完成した制御面側をもとにする方法等）考えられる。パナールとしてこの制御面側を再構成し、無線区間に「パナールサブユニット」としてこれを公開する方法が考えられる。この場合には、代理デコーダ208には、このパナール、DDIで生成されるべきHAV1やAV/CFのコンテキスト（中継ノード4102から送信ノード4101に対して実行される）の再デコーダが用意されることとなる。この方法は、無線ノード4103内にHAV1パイプラインの仮想マシンが存在

ードにてコンテントデータの暗号の復号化、および再暗号化を行なう必要が無いような方法の説明を行なう。すなわち、第2の実施形態では、到着したデータについて、中継ノードにてIEEE1394区間の暗号の復号化を行い、無線区間の暗号化を再実行するという手順を繰り返す。これに対し、第6の実施形態では、IEEE1394バス側から到着した暗号化データをそのまま無線網上に転送するような方法である。

[0225] 図77に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的に第2の実施形態と同様である。

[0226] 図78に、送信ノード9101の内部構造の一例を示す。これも第2の実施形態と基本的には同様である。認証ソフトウェアが、ノードに一つ用意されている。

[0227] 図79に、中継ノード9102の内部構造の一例を示す。認証ソフトウェアが、Ceer、Ceer、ネットワークアダプタ、IEEE1394側にBceer、無線網側にCeer) 用意されている。IEEE1394側のISO暗号送受信部9203と無線ISO暗号送受信部9206間で、(復号化/暗号化のフローを遂行)して直接暗号化されたストリーム暗号を取り取りされる点を除いて、第2の実施形態と同様である。

[0228] 図80に、無線ノード9103の内部構造の一例を示す。これも第2の実施形態と基本的には同様である。認証ソフトウェアが、ノードに一つ用意されている。

[0229] これまでの実施形態と同様に、中継ノードでは、IEEE1394側には無線網上のサービス、無線網側にはIEEE1394上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

[0230] 次に、本実施形態の全体のシーケンス例を図81に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス(映像送信サブユニット)を代理で無線網側に広告しており、無線ノード(映像送信サブユニット)が、中継ノードの代理機能に対してサービス(MPEG映像伝送要求)を要求、中継ノードが映像のサービスを提供して、送信ノードの映像送信サブユニットに対して、映像の映像伝送要求を行う。実際の映像データは、暗号化された形でIEEE1394上は同期チャネル上に、無線網上は無線同期チャネル上に転送されるものとする。なお、詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

[0231] また、送信ノード9101の動作手順例を図82に、中継ノード9102の動作手順例を図83、図84に、無線ノード9103の動作手順例を図85、図86に、それぞれ示す。

[0232] 本実施形態では、IEEE1394上の著作権保護方式である「SC Digital Transmission Content Protection Specification」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。なお、本実施形態では、認証・鍵交換方式をノード単位で行う場合について説明する(サブユニット単位で行う場合については、第7の実施形態で説明する)。

[0233] さて、送信ノード9101は、IEEE1394の同期チャネル上に、コンテント鍵Kで暗号化されたMPEG映像を転送する(ステップS8501、S8601、S8701)。これを受信した中継ノード9102は、このまま(受信したMPEG映像を、コンテント鍵Kで暗号化されたまま)無線網側の無線同期チャネル上に転送する(ステップS8509、S8701)。

[0234] 同期チャネルを通じて受信したデータが暗号化されていると認識した中継ノード9102は、到着したデータのCIPヘッダの送信ノードIDフィールド(SIDフィールド)を参照する等して、送信ノード9101と認証・鍵交換すべきであると認識する(ステップS8801)。中継ノード9102の認証ソフトウェアがBceerを含んだ認証要求パケットを送信ノード9101に対して転送する(ステップS8502、S8702)。

[0235] これを受信した送信ノード9101は、送信ノードの認証ソフトウェアがBceerを含んだ認証要求パケットを中継ノード9102に対して送信する(ステップS8503、S8602、S8603、S8703)。

[0236] 次に、認証・鍵交換手続きを行って、送信ノード9101と中継ノード9102の間で、認証鍵Kauth1を秘密鍵に共有する(ステップS8504、S8605、S8604、S8704)。

[0237] IEEE1394著作権保護方式では、コンテント鍵Kは、交換鍵Kx、シーNC、暗号暗増値EMIの3つの要素の関数Jにて計算される。すなわち、K=J(Kx, NC, EMI)である。ここでEMIは転送される暗号化データには必ず付与される値である。よって、送信ノード9101は、受信側(中継ノード)に、本実施形態の場合は無線ノード)に対して、交換鍵KxとシーNCの値を通知する必要がある。

[0238] そこで、送信ノード9101は、中継ノード9102との間で共有した認証鍵Kauth1を使って、既知の関数Jを使って、f(Kx, Kauth1)の形で中継ノード9102に送信する(ステップS8506、S8605、S8708、S8709)。中継ノード9102は、この値から、Kxの値を算出することができる。同様に、シーNCの値も、送信ノード9101から中継ノード9102に転送される(ステップS850

507、S8606、S8710)。ここで、中継ノード9102は、暗号を復号するコンテント鍵Kを生成するのに必要なKx, NCの値をこの時点で認識したことになる。

[0239] さて、同様の手続きが中継ノード9102と無線ノード9103の間でも行われる(ステップS8510~S8613、S8705~S8707、S8802~S8804)。この手続きは、送信ノード9101と中継ノード9102との間の認証・鍵交換手続きと同様である。ここでの詳細な説明は省略する。ここで、無線網の無線同期チャネル上に転送される暗号化されたデータにも、送信ノードである中継ノード9102を識別できるようにアドレス情報が付与されている。

[0240] さて、中継ノード9102と無線ノード9101とで認証鍵Kauth2が共有できたものとすると、本実施形態では、中継ノード9102は、暗号化されたMPEG映像を暗号の復号化をすることなく、そのまま無線網(の無線同期チャネル)にブロードキャストして、IEEE1394区間と無線網区間を隔てて、無線ノード9103に転送する(ステップS8507で受信したデータより算出したKx, NCのそれぞれの値を、同様に無線ノード9103に対して送信する(ステップS8614、S8615、S8709、S8711、S8805~S8807)。具体的には、Kxの値は認証鍵Kauth2の値を使ってf(Kx, Kauth2)を計算して、無線ノード9103に転出し、NCの値はそのまま転送する。

[0241] 無線ノード9103では、このようにして、中継ノードと同じ手順を使ってKx, NCの値を認識するため、同様の関数Jを使ってコンテント鍵Kの値を算出することができる(ステップS8616)。

[0242] よって、送信ノード9101から送られてくる、コンテント鍵Kで暗号化されたMPEG映像は、中継ノード9102で暗号の復号化がなされた後、そのままブロードキャストして無線ノード9103まで転送された場合(ステップS8508、S8617、S8607、S8712、S8809)でも、先にS8516で計算したコンテント鍵Kの値を使って、暗号の復号化ができる(ステップS8618、S8810)。その後、MPEG映像のデコード、ディスプレイ表示等が行われる。

[0243] なお、本実施形態では、無線網上では無線同期チャネルが定義されており、暗号化されたMPEG映像はこの無線同期チャネル上に転送されてくること

50
説明を行ってきたが、第2の実施形態のように、無線網上でのQOSデータ転送がイーサネットと同様の無線フレームを転送する場合にも、同様の方法(Kx, NCの値を無線ノードから無線ノードにブロードキャスト)が可能である。

[0244] 逆に言うと、本実施形態のような方法により、中継ノード9102では暗号の復号化および再暗号化が不要になり、復号化パケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

[0245] なお、この場合、IEEE1394側に送信ノード9102とは別のノード(別ノード)が存在しており、この別ノードから中継ノード9102を経て、無線ノード9103に別のコンテント鍵で暗号化されたデータ(秘密には同じEMI)を持ったデータを送信することはできない。コンテント鍵は、基本的にデータの送信ノード9101が決定する仕組みとなっていることから、別ノードが別のコンテント鍵を選択する可能性は十分にある。しかし、中継ノード9102と無線ノード9103との間で、既にコンテント鍵Kが一対一に定義されている。すなわち、中継ノード9102と無線ノード9103との間では、同じEMI値については、1つのコンテント鍵しか共有できない。よって、別ノード間で、高タクトのコンテント鍵しか使えない状態のため、別ノードからの(別のコンテント鍵で暗号化された)データを受信しても、これを中継ノード9102から無線ノード9103に転送する際に、別のコンテント鍵を生成できないため、これを復号化できないことになる。

[0246] よって、中継ノード9102は、既に暗号化データを転送しているノード(本実施形態の場合、無線ノード9103)に対して、別のコンテント鍵を使う必要のある暗号化データの送信要求があった場合(例えば、IEEE1394の別ノードの代理サービスに対するサービス要求があった場合等)は、これを拒否することにより、未然に上記矛盾を回避することが可能となる。また、中継ノード9102は、既に無線ノード9103に対して暗号化データの送信を行っている場合には、該無線ノード9103に対しては、他のサービス(サブユニット)は見えない(代理サービス提供自体を中断する。あるいは暗号化ストリーム転送に伴う代理サービスの提供を中断する。等)、というやり方でも、同様の効果が考えられる。

[0247] (第7の実施形態) 第6の実施形態では、認証・鍵交換の単位を送信ノードと中継ノードの間、および中継ノードと無線ノードとでそれぞれ行ない、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いような方法であった。

[0248] これに対し、第7の実施形態では、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いのは同様であるが、無線網側の認証・鍵交換の世

51

位が、第2の実施形態と同じくサブユニット単位で
き、同じノード間でも複数のコンテンツ鍵を持つことが
できるような場合である。本実施形態によれば、IEE
E1394上の複製送信ノードからの暗号化データの同
時受信が可能となる。

【0249】図87に、ある家庭のホームネットワーク
の全体構成の一例を示す。この全体構成は、送信ノード
(PとQ)が2つある点以外、基本的に第6の実施形
態と同様である。

【0250】送信ノード9801、9811の内部構成
は、第6の実施形態と同様である。

【0251】中継ノード9802の内部構成は、IEE
E1394例では認証・鍵交換の単位がノード間であ
り、無線網側では認証・鍵交換の単位がサブユニット間
である点を除いて、第6の実施形態と同様である。

【0252】無線ノード9803の内部構成は、認証・
鍵交換の単位がサブユニット間である点を除いて、第6
の実施形態と同様である。

【0253】なお、送信ノード9801、9811、無
線ノード9802の動作手順は基本的に第6の実施形
態と同様である。また、1つの送信ノードに対して中継
を行う場合の中継ノード9803の動作手順も基本的に
は第6の実施形態と同様である。

【0254】これまでの実施形態と同様に、中継ノード
では、IEE1394例には無線網上のサブユニット、
無線網側にはIEE1394上のサブユニットのそれぞれ
で暗号化・復号機能があるものとする。なお、ここでの特
殊な説明は省略する。

【0255】次に、複数の送信ノードに対して中継を行
う場合の中継ノード9802の動作手順を図88に、
本実施形態の全体のシーケンス例を図89/図90に示
す。これまでの実施形態と同様に、例えば中継ノード
が、送信ノードが提供しているサブユニット（映像送信サ
ブユニット）を代理で無線網側に広告しており、無線ノード
F（映像デコーダサブユニット）が、中継ノードの代
理機能に対してサブユニット（MPEG映像伝送要求）を要
求、中継ノードが要求のサブユニットを提供している送信ノ
ードの映像送信サブユニットに対して、実際の映像伝送
要求を行う。実際の映像データは、暗号化された形でIEE
E1394上は同期チャネル#x上を、無線網上は
無線網同期チャネル#y上を伝送されるものとする。詳細
はこれまでの実施形態と同様であるので、ここでの詳細
な説明は省略する。

【0256】本実施形態でも、IEE1394上の音
作保護方式である「SC Digital Trans
mission Content Protection
on Specification」の認証・鍵交換方式
に基本的に準ずる手順を踏むものとする。
【0257】さて、送信ノードP（9801）は、IEE
E13944の同期チャネル#x上に、コンテンツ鍵K

52

1で暗号化されたMPEG映像を伝送する（スレッツS
9201、S9301）。第6の実施形態と同様に、コ
ンテンツ鍵K1は、K1=J（KxP、NcP、Em
1）にて計算されるものとする。これを受信した中継ノ
ード9802は、このまま（受信したMPEG映像を、
コンテンツ鍵K1で暗号化したまま）無線網側の無線
網同期チャネル#yに対して伝送する（スレッツS920
9、S9301）。

【0258】中継ノード9802が送信ノードPに対し
て認証要求し、鍵交換を行って、交換鍵KxPと
シードNcPを獲得する手順（スレッツS9202～S
9207、S9302）は、第6の実施形態と同様であ
るので、ここでの詳細な説明は省略する。この時点で、
中継ノード9802は暗号を復号するために必要なKx
P、NcPの値を認識したこととなる。

【0259】さて、同様の認証・鍵交換手続きが中継ノ
ード9802と無線ノード9803の間で行われる
（スレッツS9210～S9217、S9303）。こ
の手続きは第2の実施形態の送信ノードと中継ノード間
の認証・鍵交換手続きと同様であるので、ここでの詳細
な説明は省略する。ただし、認証先明い合わせや認証先
番号、あるいは認証要求にサブユニットのIDの他、チ
ャネル番号、あるいは暗号化データの送受信を行うこと
になるサブユニットの識別子をお知らせして、これを行ってよ
い、中継ノード9802、あるいは無線ノード9803
が、「1つの暗号化データについての認証・鍵交換手続き
か」ということと識別できるようになり、後述するよう
に、異なる種類の暗号化データについては、同一ノード
間の認証・鍵交換であったとしても、異なる鍵を通知す
ることが可能になる。

【0260】なお、この際、認証要求にチャネル番号を
含める場合は、スレッツS9210の認証先明い合わせ
とスレッツS9211の認証先番号は不要となる。
【0261】さて、中継ノード9802と無線ノード9
803で認証鍵Kauth1が共有できたものとする。
本実施形態でも、中継ノード9802は、暗号化された
MPEG映像を自身の復号化をすることなく、そのまま
無線網（の無線網同期チャネル#y）にブロードキャスト
行ってしまうため、中継ノード9802は無線ノード9
803に対して、交換鍵KxPとシードNcPの値を通知
する必要がある（逆に通知できれば、無線ノード98
03は暗号の復号が可能である）。そこで、中継ノード
9802は、S9206、S9207で受信したデー
タより算出したKxP、NcPのそれぞれの値を、同様に
無線ノード9803に対して送信する（スレッツS9
216、S9217）。KxPの値は認証鍵Kauth
1の値を使って（KxP、Kauth1）を計算し
て、無線ノード9803に送出する（スレッツS921
6）。

【0262】無線ノード9803では、このようにし

53

て、中継ノード9802と同じ手順を使ってKxP、N
cPの値を認識できるため、同様の関数Jを使ってコン
テンツ鍵K1の値を算出することができる（スレッツS
9218）。

【0263】よって、送信ノードPから送られてくる、
コンテンツ鍵K1で暗号化されたMPEG映像は、中継
ノード9802で暗号の復号化をせずに、そのままブ
ロードして無線ノード9803まで伝送されてきた場合
（スレッツS9208、S9219）でも、先にスレッ
ツS9218で計算したコンテンツ鍵K1の値を使っ
て、暗号の復号化ができる（スレッツS9220）。そ
の後、MPEG映像のデコード、ディスプレイ表示等が
行われる。

【0264】本実施形態のような方法でも、中継ノード
9802では暗号の復号化、および暗号化が不要にな
り、高速なパケット伝送も可能になることから、低コス
トな中継ノードの構築が可能となる。

【0265】さて、次に、別の送信ノードQ（981
1）が、同時に中継ノード9802を介して無線ノード
9803に対して別のコンテンツ鍵K2で暗号化された
データを伝送する場合（スレッツS9221、S922
9、S9304）を考える。

【0266】本実施形態の前半と同様に、送信ノードQ
と中継ノード9802との間で認証・鍵交換が行われ
（スレッツS9222～S9227）、中継ノード98
02は交換鍵KxQとシードNcQの値をそれぞれ得る
ことが可能となる。

【0267】本実施形態においては、中継ノード980
2と無線ノード9803との間の認証は、サブユニット
間単位であるので、暗号化データの送受信が既にあるサブユ
ニット間で行われているものとする。中継ノード98
02と無線ノード9803との間で複製の認証・鍵交換
が可能となる。

【0268】すなわち、本実施形態の前半と同様に、中
継ノード9802と無線ノード9803との間で、本実
施形態の前半とは異なるサブユニット間で認証・鍵交換
を行っていく（スレッツS9230～S9235、S9
305）。その上で、中継ノード9802は、送信ノ
ードQと自ノード（中継ノード）9802との間の交換鍵
KxQとシードNcQを、無線ノード9803にブロード
キャストする（スレッツS9236、S9237、S930
5、S9306）。

【0269】無線ノード9803では、このようにし
て、KxQ、NcQの値を認識できるため、同様の関数
Jを使ってコンテンツ鍵K2の値を算出することができ
る（スレッツS9238）。

【0270】よって、送信ノードQから送られてくる、
コンテンツ鍵K2で暗号化されたMPEG映像は、中継
ノード9802で暗号の復号化をせずに、そのままブ
ロードして無線ノード9803まで伝送されてきた場合

54

（スレッツS9228、S9229）でも、先にスレッ
ツS9238で計算したコンテンツ鍵K2の値を使っ
て、暗号の復号化ができる（スレッツS9240）。つ
まり、2つの異なるコンテンツ鍵（本実施形態ではK1
とK2）で暗号化されたMPEG映像の同時受信が可能
となる。

【0271】なお、第6の実施形態と第7の実施形態で
は、IEE1394と無線網との相互接続を行う場合
を別に説明してきたが、インターネット等の他の網
についても適用可能である。

【0272】なお、第1～第7の実施形態において例示
したデータ伝送の方向とは逆の方向にデータ伝送する場
合（例えば、無線ノードPからIEE1394上のノー
ドへデータ伝送する場合）にも、本発明は適用可能であ
る。

【0273】また、第1～第7の実施形態において、無
線ノードPとIEE1394上のノードについては、コ
ンテンツ鍵について送受信された受信機能の一方に着目
して説明したが、無線ノードPやIEE1394上のノー
ドは、コンテンツについて送受信機能と受信機能の両方
を備えることも可能である。

【0274】また、認証手続きや、鍵交換手続き（コン
テンツ鍵共有手続き）は、これまで例示したものに限
定されず、他の組の方法が用いられる場合にも本発明
は適用可能である。

【0275】また、以上では、家庭ネットワークとし
て実施形態を説明したが、もちろん、本発明は家庭網以
外のネットワークにも適用可能である。

【0276】なお、以上の各機能は、ソフトウェアとし
ても実現可能である。

【0277】また、本実施形態は、コンピュータに所定
の手段を実行させるための（あるいはコンピュータを所
定の手段として機能させるための、あるいはコンピュータ
に所定の機能を実現させるための）プログラムを記録
したコンピュータ読取り可能な記録媒体としても実施す
ることができる。

【0278】本発明は、上述した実施形態に限定され
るものではなく、その技術的範囲において種々変形して
実施することができる。

【0279】
【発明の効果】本発明によれば、同じネットワークでは
接続されていない装置間で、保護すべきコンテンツの送
受信のためのコンテンツ保護方式を行うことが可能に
なる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るネットワークの
全体構成の一例を示す図
【図2】送信ノードの内部構造の一例を示す図
【図3】中継ノードの内部構造の一例を示す図
【図4】無線ノードの内部構造の一例を示す図

- 【図5】全体のシーケンスの一例を示す図
【図6】全体のシーケンスの一例を示す図
【図7】送信ノードの動作手順の一例を示すフローチャート
【図8】送信ノードの動作手順の一例を示すフローチャート
【図9】中継ノードの動作手順の一例を示すフローチャート
【図10】中継ノードの動作手順の一例を示すフローチャート
【図11】中継ノードの動作手順の一例を示すフローチャート
【図12】無線ノードの動作手順の一例を示すフローチャート
【図13】無線ノードの動作手順の一例を示すフローチャート
【図14】無線ノード構成情報バケットの一例を示す図
【図15】代理テーブルの一例を示す図
【図16】代理テーブルの一例を示す図
【図17】送信ノードから見た中継ノードの内部構造を説明するための図
【図18】無線ノードから見た中継ノードの内部構造を説明するための図
【図19】無線ノード制御バケットの一例を示す図
【図20】本発明の第2の実施形態に係るネットワークの全体構成の一例を示す図
【図21】送信ノードの内部構造の一例を示す図
【図22】中継ノードの内部構造の一例を示す図
【図23】無線ノードの内部構造の一例を示す図
【図24】全体のシーケンスの一例を示す図
【図25】全体のシーケンスの一例を示す図
【図26】送信ノードの動作手順の一例を示すフローチャート
【図27】送信ノードの動作手順の一例を示すフローチャート
【図28】中継ノードの動作手順の一例を示すフローチャート
【図29】中継ノードの動作手順の一例を示すフローチャート
【図30】中継ノードの動作手順の一例を示すフローチャート
【図31】中継ノードの動作手順の一例を示すフローチャート
【図32】無線ノードの動作手順の一例を示すフローチャート
【図33】無線ノードの動作手順の一例を示すフローチャート
【図34】代理テーブルの一例を示す図
【図35】代理テーブルの一例を示す図
【図36】送信ノードから見た中継ノードの内部構造を

- 説明するための図
【図37】無線ノードから見た中継ノードの内部構造を説明するための図
【図38】無線フレームのフォーマットの一例を示す図
【図39】無線制御バケットのフォーマットの一例を示す図
【図40】本発明の第3の実施形態に係るネットワークの全体構成の一例を示す図
【図41】送信ノードの内部構造の一例を示す図
【図42】中継ノードの内部構造の一例を示す図
【図43】無線ノードの内部構造の一例を示す図
【図44】全体のシーケンスの一例を示す図
【図45】全体のシーケンスの一例を示す図
【図46】送信ノードの動作手順の一例を示すフローチャート
【図47】送信ノードの動作手順の一例を示すフローチャート
【図48】中継ノードの動作手順の一例を示すフローチャート
【図49】中継ノードの動作手順の一例を示すフローチャート
【図50】中継ノードの動作手順の一例を示すフローチャート
【図51】無線ノードの動作手順の一例を示すフローチャート
【図52】無線ノードの動作手順の一例を示すフローチャート
【図53】代理テーブルの一例を示す図
【図54】代理テーブルの一例を示す図
【図55】送信ノードから見た中継ノードの内部構造を説明するための図
【図56】無線ノードから見た中継ノードの内部構造を説明するための図
【図57】無線ノードに送られてきた制御画面の一例を示す図
【図58】本発明の第4の実施形態に係るネットワークの全体構成の一例を示す図
【図59】送信ノードの内部構造の一例を示す図
【図60】ホムゲートウェイの内部構造の一例を示す図
【図61】受信ノードの内部構造の一例を示す図
【図62】全体のシーケンスの一例を示す図
【図63】全体のシーケンスの一例を示す図
【図64】送信ノードの動作手順の一例を示すフローチャート
【図65】送信ノードの動作手順の一例を示すフローチャート
【図66】ホムゲートウェイの動作手順の一例を示すフローチャート
【図67】ホムゲートウェイの動作手順の一例を示す

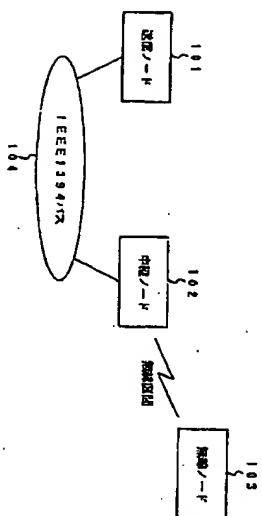
- フローチャート
【図68】ホムゲートウェイの動作手順の一例を示すフローチャート
【図69】ホムゲートウェイの動作手順の一例を示すフローチャート
【図70】受信ノードの動作手順の一例を示すフローチャート
【図71】受信ノードの動作手順の一例を示すフローチャート
【図72】送信ノードのペネルとホムゲートウェイの送信ノード制御用ホムページの一例を示す図
【図73】本発明の第5の実施形態に係るネットワークの全体構成の一例を示す図
【図74】ホムゲートウェイの内部構造の一例を示す図
【図75】全体のシーケンスの一例を示す図
【図76】制御画面の一例を示す図
【図77】本発明の第6の実施形態に係るネットワークの全体構成の一例を示す図
【図78】送信ノードの内部構造の一例を示す図
【図79】中継ノードの内部構造の一例を示す図
【図80】無線ノードの内部構造の一例を示す図
【図81】全体のシーケンスの一例を示す図
【図82】送信ノードの動作手順の一例を示すフローチャート
【図83】中継ノードの動作手順の一例を示すフローチャート
【図84】中継ノードの動作手順の一例を示すフローチャート
【図85】無線ノードの動作手順の一例を示すフローチャート
【図86】無線ノードの動作手順の一例を示すフローチャート
【図87】本発明の第7の実施形態に係るネットワークの全体構成の一例を示す図
【図88】中継ノードの動作手順の一例を示すフローチャート
【図89】全体のシーケンスの一例を示す図
【図90】全体のシーケンスの一例を示す図
【符号の説明】
101, 2101, 4101, 6101, 8101, 9101, 9801, 9811...送信ノード
102, 2102, 4102, 6102, 8102, 9802...中継ノード
103, 2103, 4103, 6104, 9103, 9803...無線ノード
6102, 8102, 8103...ホムゲートウェイ
6103, 8104...受信ノード
104, 2104, 4104, 8105, 8107, 9104, 9804...IEEE1394バス

- 6105, 8106...公衆網
201, 2201, 4201, 6201, 8201, 9101...IEEE1394インフラエース
202, 2202, 4202, 6202...無線インフラエース
203, 2207, 4203, 6207, 8203, 9207...AV/ビデオ処理部
204, 2203, 4204, 6203, 8204, 9203...ISO符号送受信部
205, 2206, 4205, 6206...無線ISO符号送受信部
206, 2209, 4206, 6209, 9209...1394バス構成認識部
207, 2210, 4207, 8207, 9210...代理ユニキャスト構成部
208, 2214, 4208, 6215, 9214...代理テーブル
209, 2211, 4209, 9211...無線区間構成認識部
210, 4210, 8209...ビデオテラクション制御ソフトウェア部
2208, 6208...IEEE1394コピテラクション処理部
2212, 9212...無線区間コピテラクション部
2211...変換テーブル
211, 2213, 4211, 9213...無線ノード制御バケット送受信部
2204, 6204...符号番号化部
2205, 6205...符号化部
4212...HAVI処理部
4213...IEEE1212レジスタ
6206, 8205...AV信号送受信部
6202, 8202...インターネットエース
6210, 8208...代理ホムページ作成部
6211, 8210...ホムページ作成・管理部
6212...インターネット制御テラクション処理部
6213...制御バケット送受信部
6214...MPEG2/MP EG4変換部
6206...制御バケット処理部
301, 2301, 4301, 9301...無線インフラエース
302, 2302, 4302, 9302...無線ノード制御バケット送受信部
303, 2303, 4303, 6303, 9303...ビデオテラクション処理部
304, 2304, 4304, 9304...無線ISO符号送受信部
305, 2305, 4305, 6305, 9305...符号番号化部
306, 2306, 4306, 6306, 9306...M

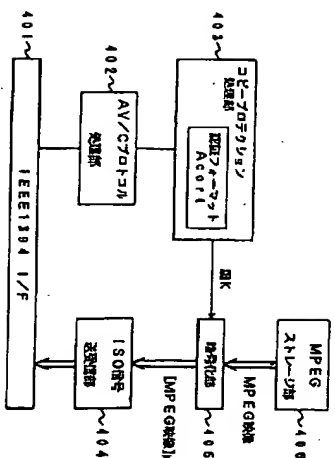
PEGコード部
307, 2307, 4307, 6307, 9307...
スプレッド部
6301...インターネットインタフェース
6302...制御/ネット送受信部
6304...AV信号送受信部
401, 2401, 4401, 6401, 9401...
EEE1394インタフェース
402, 2402, 4402, 6402, 9402...
V/Cプロセッサ部

*403, 2403, 4403, 6403, 9403...
ビデオデジタイザ部
404, 2404, 4404, 6404, 9404...
SO信号送受信部
405, 2405, 4405, 6405, 9405...
増幅部
406, 2406, 4406, 6406, 9406...
PEGスプレッド部
4407...EEE1212レジスタ

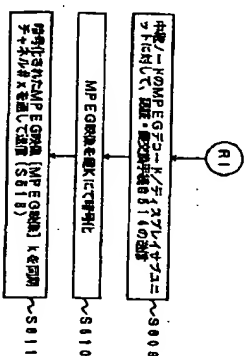
【図1】



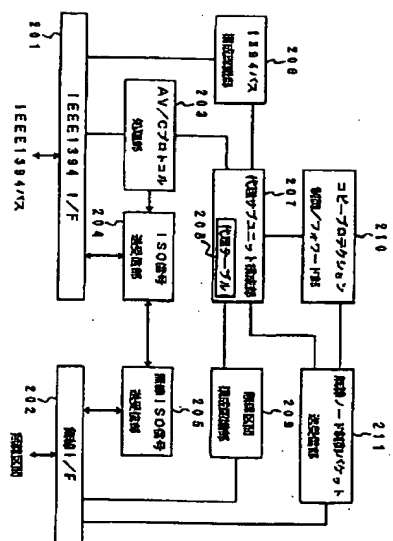
【図2】



【図3】

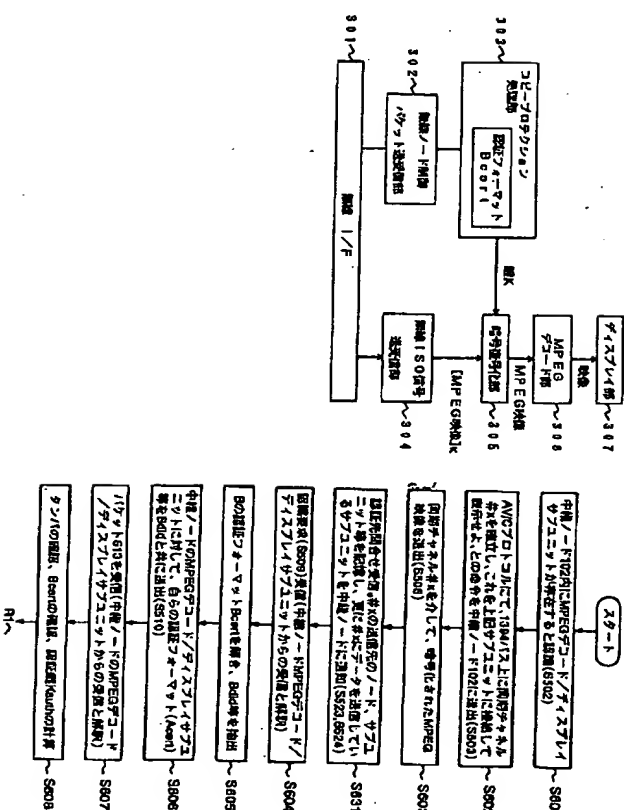


【図3】

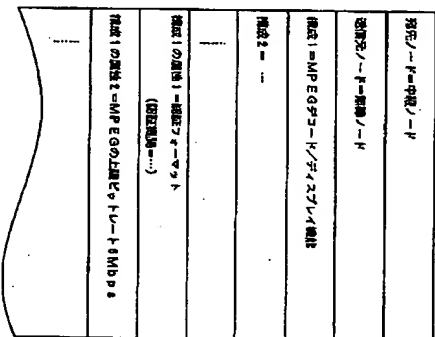


【図4】

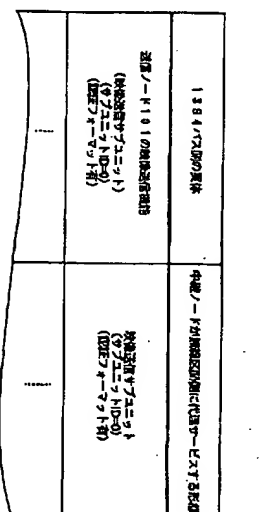
【図7】



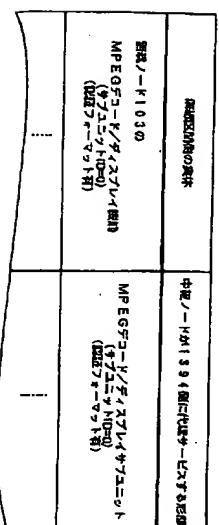
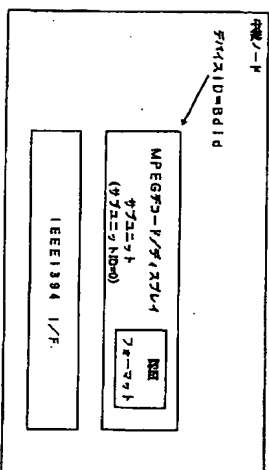
【图 38】



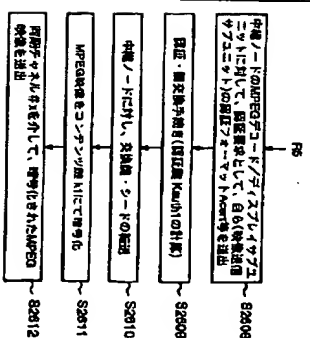
【61図】



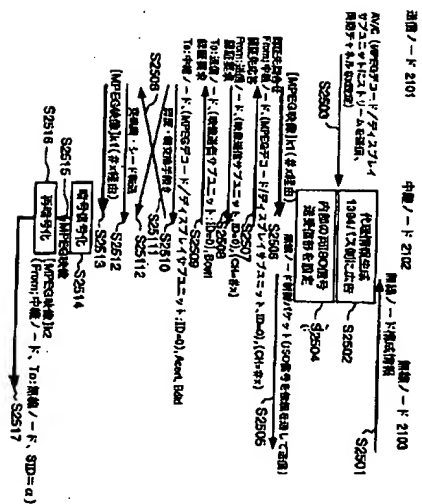
—



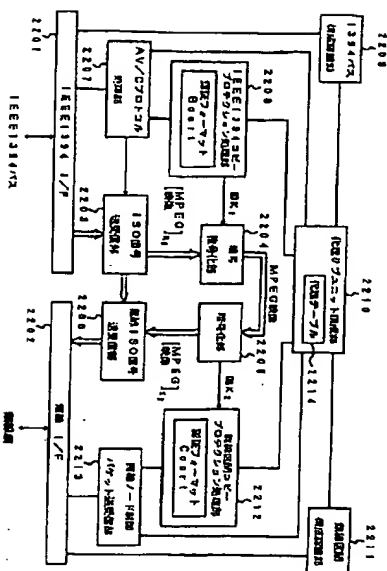
【例 27】



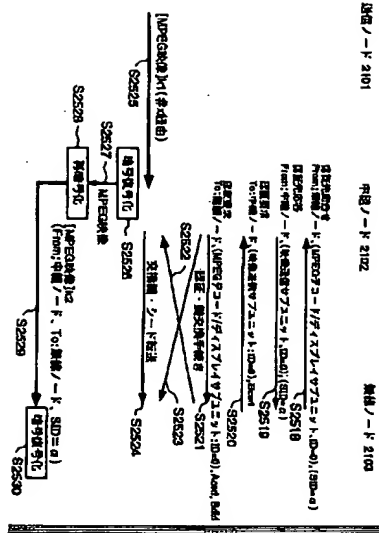
【圖 24】



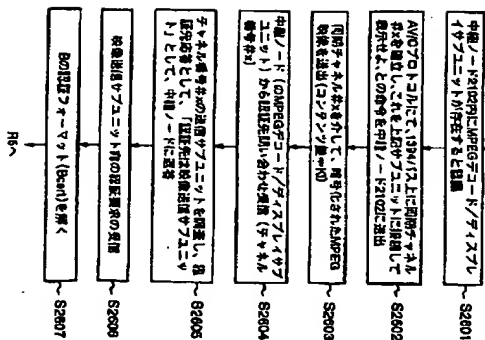
【圖 3 1】



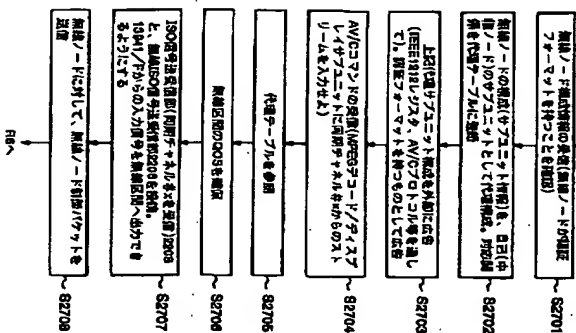
【図25】



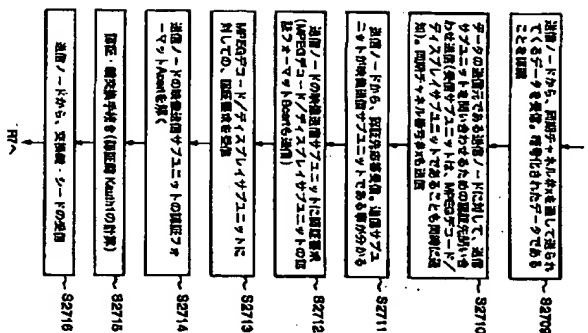
【図26】



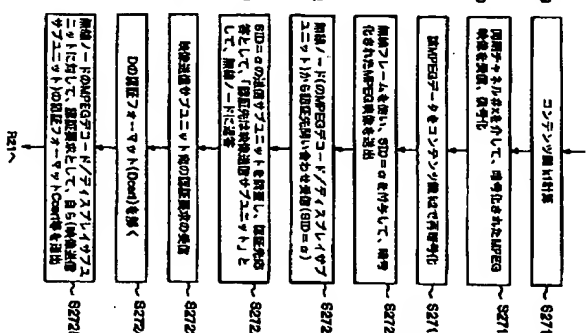
【図28】



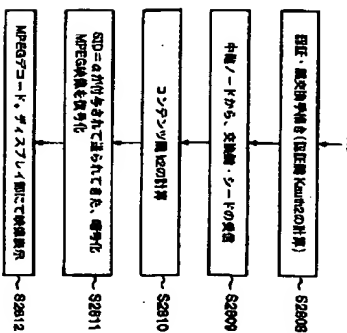
【図29】



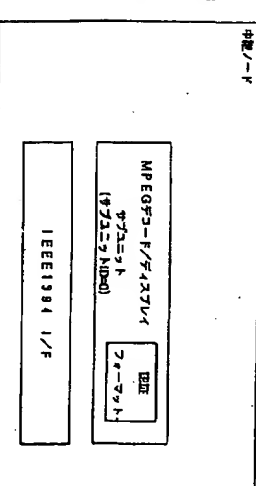
【図30】



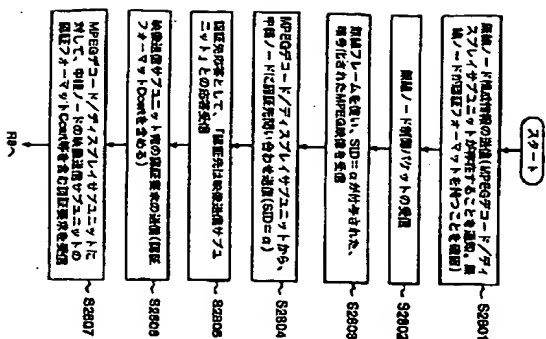
【図33】



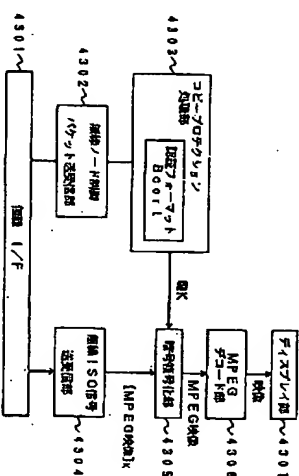
【図36】



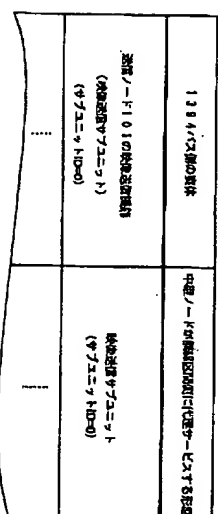
【例 3 2】



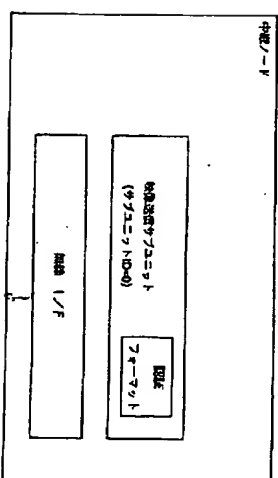
【图 43】



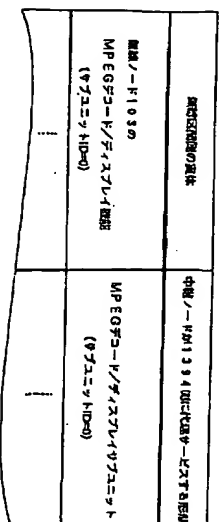
【图 3-5】



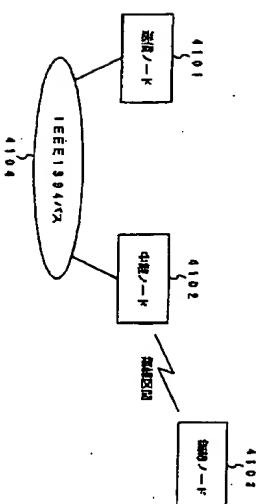
【圖 37】



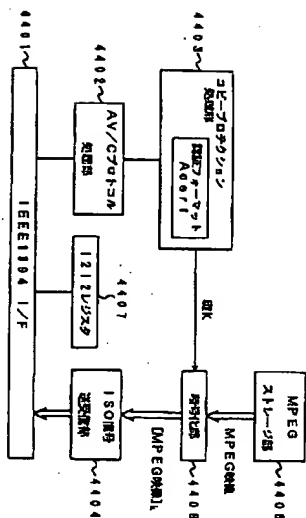
【図34】



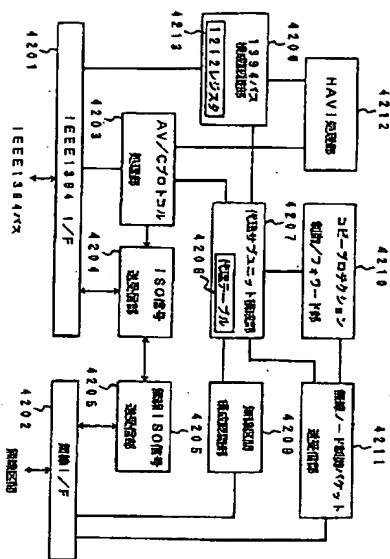
【圖40】



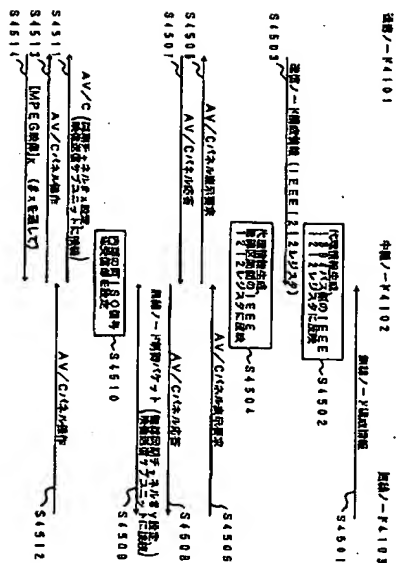
【図41】



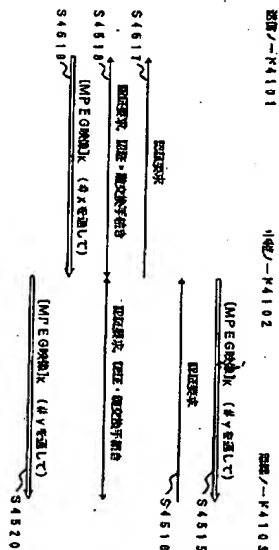
【図42】



【図44】



【図45】



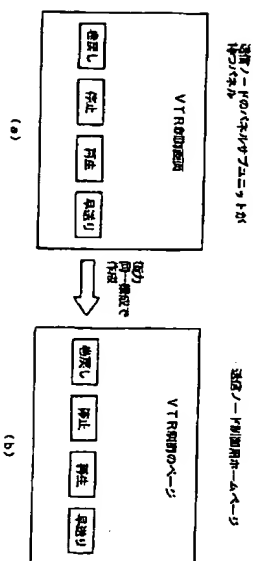
【図53】

無線LANの媒体	中継ノード1104側に代送ユーザする距離
無線ノード11030	MPEGコア/チキシル/チキシルユニット (送信ユーザ側)
無線ノード11031の代送媒体	パナリユニット

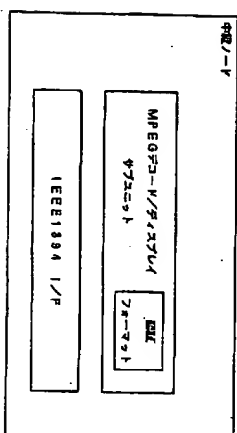
【図54】

1104ノードの媒体	中継ノード1104側に代送ユーザする距離
無線ノード1101の代送媒体ユニット (送信ユーザ側)	無線送信ユニット (送信ユーザ側)
無線ノード1101の代送媒体ユニット	パナリユニット

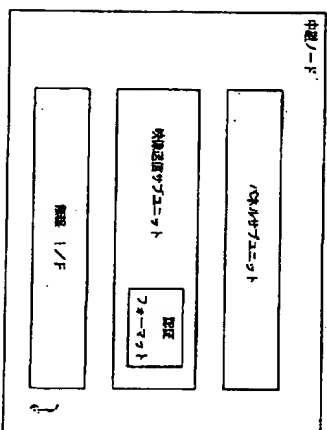
【図72】



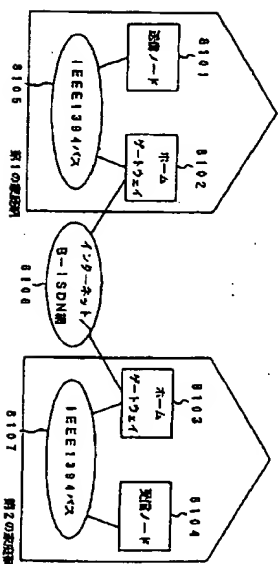
【図55】



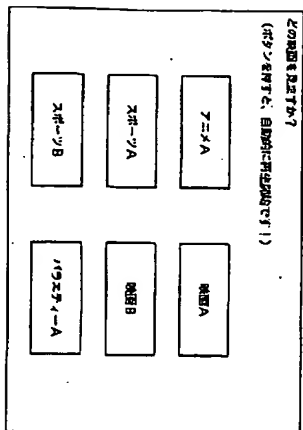
【図56】



【図73】



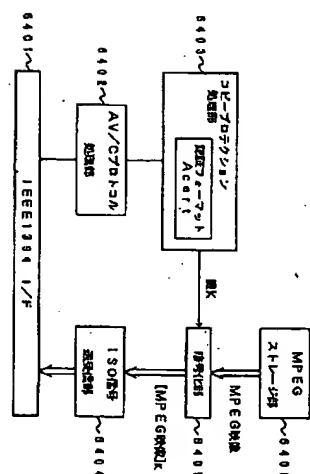
【図57】



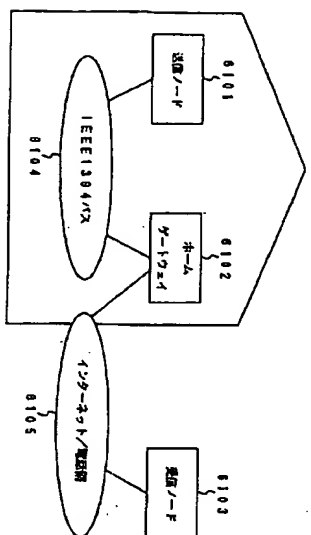
【図65】



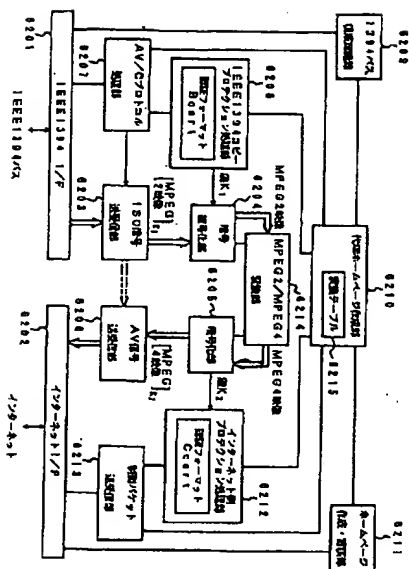
【図59】



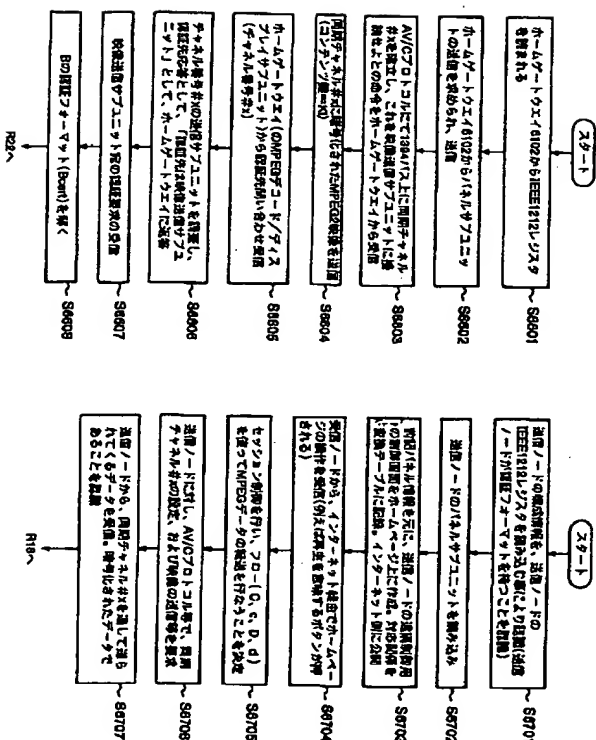
【図58】



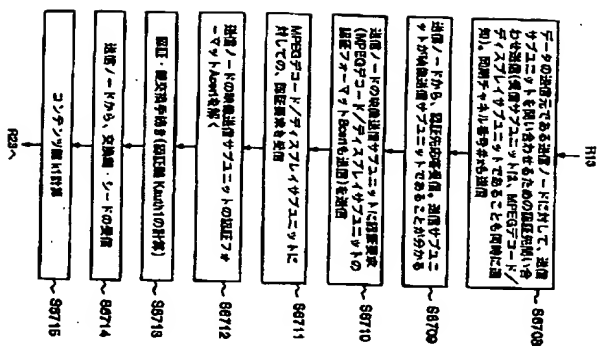
【図60】



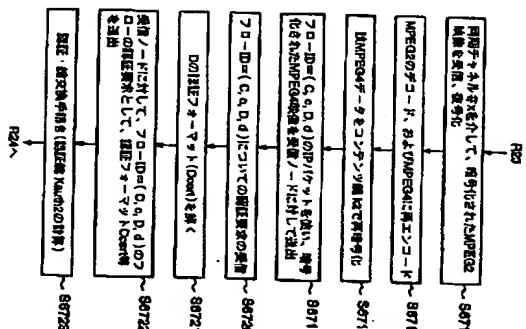
【图 6-6】



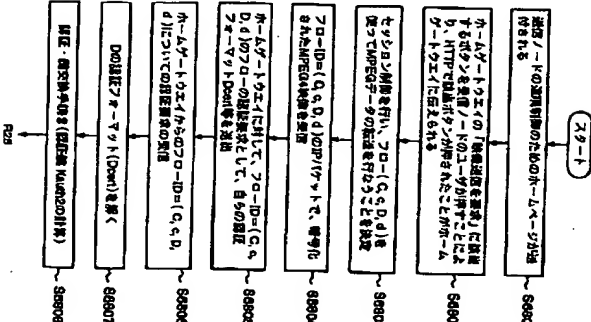
【図67】



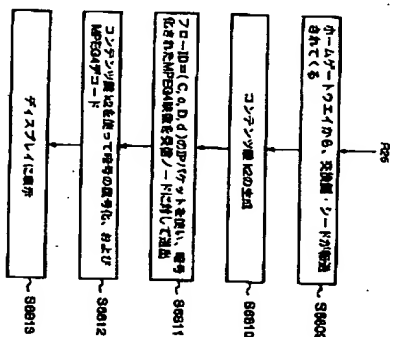
【図68】



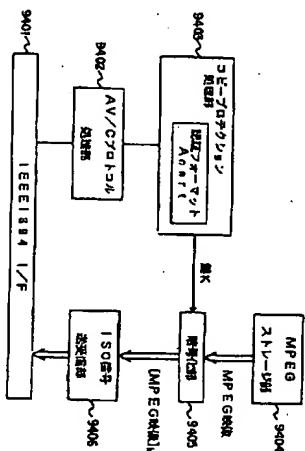
【図70】



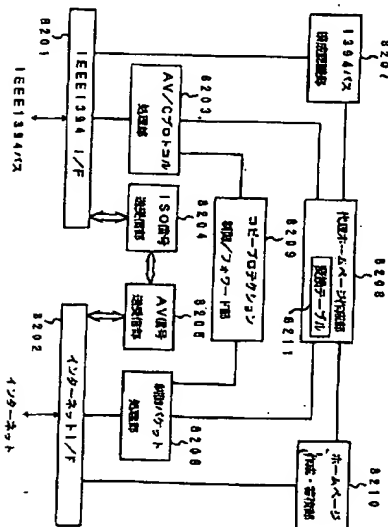
【図71】



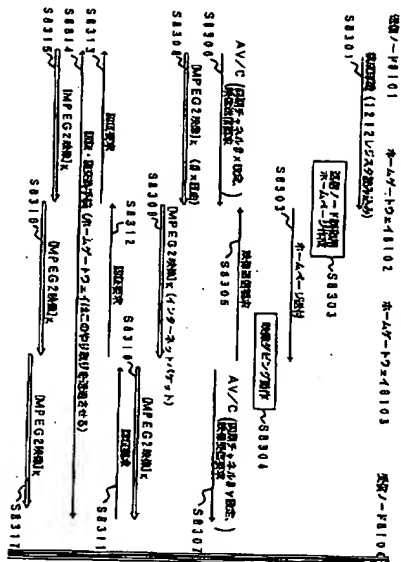
【図78】



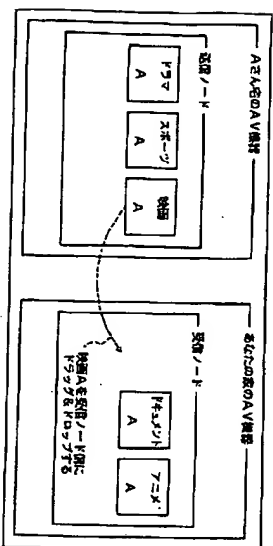
【図74】



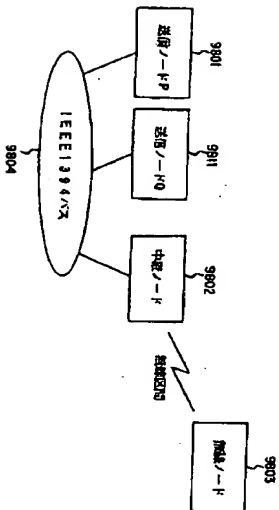
【図75】



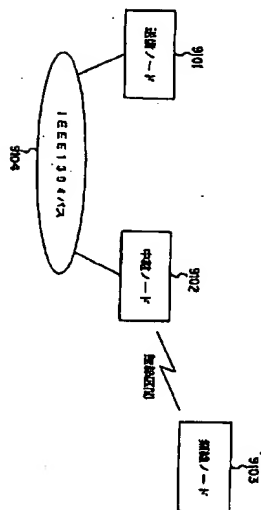
【図76】



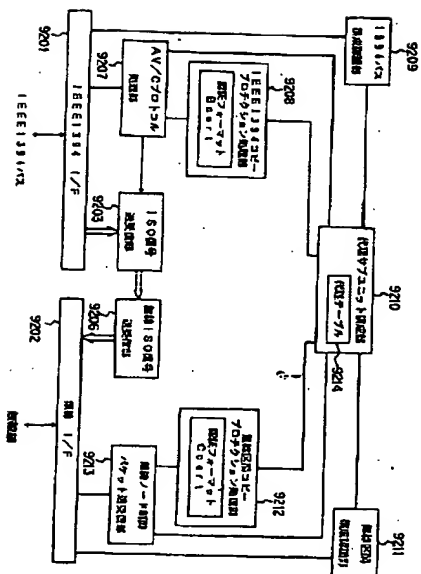
【図77】



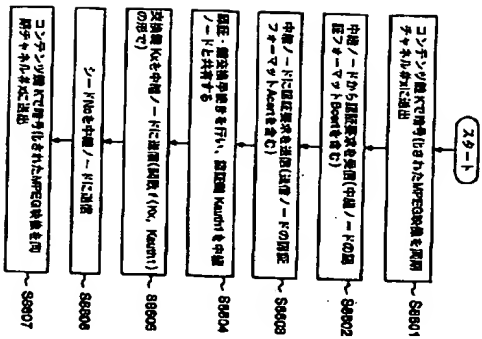
【図77】



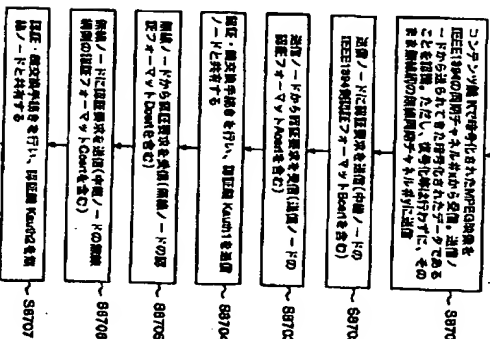
【図79】



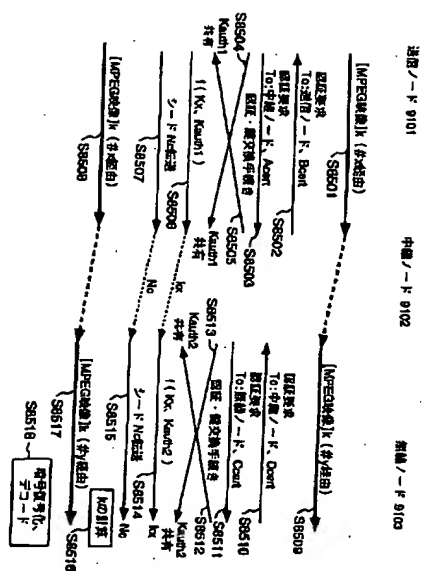
【圖 82】



29-1



【例85】



【図 85】

